Yksityisyys ja henkilötiedot www-sivustoilla

Paula Silvennoinen

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Pro gradu -tutkielma
Lokakuu 2004

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Silvennoinen, Paula: Yksityisyys ja henkilötiedot www-sivustoilla
Pro gradu -tutkielma, 58 sivua
Lokakuu 2004

Tutkielmassa esitellään henkilötietojen käsittelyä koskeva lainsäädäntö, sen tausta ja perusperiaatteet, joita henkilötietojen käsittelyssä tulee noudattaa. Tarkastelussa keskitytään erityisesti Internet-palveluiden toteutustapoihin. Työssä kerrotaan myös, millaisia henkilötietojen hyödyntämismahdollisuuksia tietojenkäsittelyn kehitys on rekisterinpitäjille tuonut. Lopuksi kuvaillaan tapoja ja teknisiä keinoja, joilla yksityisyyttä voidaan Internetissä tukea.

Avainsanat: yksityisyys, tietosuoja, henkilötiedot, www-sivustot, eväste.

Sisällys

1. Johdanto

Henkilötietojen käsittely on kokenut viime vuosina suuren muutoksen. Käsittely on muun muassa yleistynyt ja muuttunut tavanomaisemmaksi verkkosivustojen ryhdyttyä tarjoamaan palveluja, joissa rekisteröidään yksityisten henkilöiden tietoja. Tietoverkoissa myös rekisteröity voi aiempaa konkreettisemmin osallistua rekisterinpitoon ja jopa ylläpitää itse omia tietojaan. Henkilötietojen käsittely ei kuitenkaan ole sääntelemätöntä toimintaa, joten siinä tulisi — käsittely-ympäristöstä riippumatta — noudattaa henkilötietolakia ja muuta tietosuojalainsäädäntöä. Vaikka Suomessa henkilötietojen käsittelyä koskeva lainsäädäntö on ollut voimassa jo 1980-luvulta alkaen, useimmille verkossa toimiville rekisterinpitäjille lakisääteiset velvoitteet tulevat yhä edelleen täytenä yllätyksenä.

Verkkosivustojen kautta tapahtuva rekisterinpito aiheuttaa haasteita myös tietosuojalainsäädännölle. Tietoverkkojen aikana voidaan pohtia muun muassa sitä, voiko rekisterinpitäjä edes toteuttaa sille osoitetut velvoitteet henkilötietojen ajantasaisuudesta ja virheettömyydestä, kun aloite rekisteriin tallennettavista tiedoista on alunperinkin saattanut tulla rekisteröidyn taholta? Omat ongelmansa aiheuttavat verkossa liikkumisesta jäävät sähköiset jalanjäljet, joiden jättämisestä käyttäjä ei useimmiten voi olla tietoinen. Jälkiä kuitenkin kerätään esimerkiksi hallinnollisiin tai kaupankäynnin tietokantoihin valvonta- tai markkinointitarkoituksia varten. Sähköiset jalanjäljetkin ovat henkilötietoja, mikäli niiden jättäjä on tietojen perusteella tunnistettavissa.

Tutkielmassa tarkastellaan tavanomaisia, henkilötietoja käsitteleviä www-sivustoja, kuten verkkolehtiä, verkkokauppoja ja julkisen hallinnon tarjoamia palveluita — esimerkkinä vaikkapa TV-luvan käyttöönotto- tai irtisanominen. Työ ei käsittele yritysten sisäisiä tietoverkkoja tai jonkin erityislainsäädännön piiriin kuuluvia, esimerkiksi sosiaali- ja terveydenhuoltoalan palveluita. Tutkielman tarkoittamia verkkosivustoja ovat siis Internetin kautta, lähinnä selainohjelmalla käytettävissä olevat, yleiseen käyttöön suunnatut palvelut. Työssä esitellyt periaatteet soveltuvat kuitenkin yhtä hyvin esimerkiksi mobiililaitteiden kautta käytettäviin verkkopalveluihin.

Henkilörekisterilain voimassaolon aikana puhuttiin henkilörekistereistä — nykylainsäädäntö on kuitenkin laajentunut pelkästä rekisterinpidosta kaikkeen henkilötietojen automaattiseen käsittelyyn. Tutkielman käsitteistössä puhutaan rekisteröidyistä ja vastaavasti rekisterinpitäjistä. Osaksi nämä käsitteet ovat henkilörekisterilain peruja, mutta toisaalta automaattinen henkilötietojen käsittely kohdistuu edelleenkin useimmiten juuri rekistereihin tai niiden osiin. Kannattaa huomata, että sähköisen viestinnän tietosuojalaissa verkkopalvelulla tarkoitetaan "teleyrityksen toteuttamaa viestintäverkon tarjoamista käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon etukäteen rajoittamattomalle käyttäjäpiirille" [SVTSL 2 §]. Tässä työssä verkkopalveluilla tarkoitetaan kuitenkin eri asiaa, eli www-sivustoilla tarjolla olevia palveluita.

1.1. Tietosuoja — ongelmasta perusoikeudeksi

Suomessa tietosuojalainsäädäntö on joskus nähty turhana ja jopa tiedonsaannin rajoittamisena [Korpela, 2003b]. Tietosuojaa ei ole pidetty tarpeellisena eikä sen perimmäistä tarkoitusta, henkilöitten yksityisyyden suojaamista, ole ymmärretty. Sen sijaan tietosuoja on mielletty kirjaimellisesti *tietojen* suojaamisena. Lisäksi vallalla on tuntunut olevan asenne, jonka mukaan rehellisellä ihmisellä ei pitäisi olla mitään salattavaa, joten tietosuojallakaan ei siten ole virkaa [Partanen, 1995].

Tietosuojaviranomaisten kannanotot ja muiden tahojen mielipiteet ovat usein olleet vastakkaisia. Avointen tietoverkkojen ja henkilökohtaisten tietokoneitten yleistyttyä 1990-luvulla tietosuojavaltuutettua on syytetty jopa Internetin sensuroimisen yrityksestä [Kuopus, 1995]. Ikävästä maineestaan huolimatta tietosuojaviranomaiset ovat sitkeästi koettaneet tuoda esiin näkemystä, jonka mukaan tietosuojalainsäädännössä on kyse henkilötietojen käsittelyn oikeuttamisesta, ei sen rajoittamisesta [Kuopus, 1995; Partanen, 1995].

On myös uhottu, ettei tietoverkkojen aikakaudella ole enää yksityisyyttä. Yhteiskunnan muuttumisprosessia arvioitaessa yksityisyyden suoja on kuitenkin haluttu nimenomaan kirjata mukaan hallitusmuotoon perusoikeusuudistuksen yhteydessä. Yksityiselämän suoja on siis yhteiskuntamme arvoista kertova perusoikeus. Tietosuojalainsäädäntöön kuuluvan henkilötietolain valmistelutöissä [HE 96/1998] lainsäätäjä on todennut: "Yksilön oikeus itseään koskeviin tietoihin ilmentää länsimaisen demokratian keskeisiä arvoja, kuten oikeutta ihmisarvoiseen kohteluun, itsemääräämisoikeuteen, henkilökohtaiseen vapauteen ja yksityiselämän suojaan." Tietoverkkojen aikana oikeutta yksityisyyteen ja sen sääntelyä tarvitaankin ehkä entistä enemmän. Kuten nykyinen tietosuojavaltuutettu Reijo Aarnio [1999] on todennut, tietosuoja on tullut jäädäkseen.

1.2. Tutkielman aineiston jäsentely

Tutkielmassa esitetään aluksi aiheen keskeisimmät käsitteet, yksityisyyden suoja ja tietosuoja, sekä niiden merkitys yhteiskunnassamme yksilön oikeusturvan näkökulmasta. Sen jälkeen selvitetään tietoverkkopalveluiden kannalta olennainen tietosuojalainsäädäntö ja siitä ilmenevät periaatteet, joita henkilötietojen käsittelyssä on noudatettava. Työssä kerrotaan myös, minkälaisia oikeuksia ja velvoitteita lait eri osapuolille asettavat. Tutkielman alkuosa luo samalla katsauksen viimeisen kahdenkymmenen vuoden aikana tapahtuneeseen lainsäädännön kehitykseen. Kansallisten muutostarpeiden lisäksi tarkastellaan myös EU:n vaikutusta suomalaisen tietosuojan tasoon.

Tietosuojan teoriaosuuden jälkeen selvitetään, miten lainsäädännöstä ilmitulevia periaatteita tulisi verkkopalveluissa toteuttaa ja toisaalta kuinka sivustoja on toteutettu. Suurin osa työssä esiteltävistä käytännön esimerkeistä koskee laittomia tai huonosti tehtyjä palveluita — tämä johtuu siitä, että henkilötietolain noudattaminen verkkosivustoilla on edelleen harvinaista. Samassa yhteydessä kerrotaan tietosuojalautakunnan ja -valtuutetun tekemistä kannanotoista ja päätöksistä, jotka liittyvät tietoverkkoihin tai joita

voi niihin soveltaa. Työssä esitellään myös tietosuojavaltuutetun toimistossa tehty selvitys informointivelvoitteen täyttämisestä.

Tietoverkkojen yleistyminen on aiheuttanut uusia ilmiöitä: muun muassa rekisterinpidon luonne on muuttunut, henkilötiedoista on tullut kauppatavaraa ja kansalaisia profiloivat niin julkiset kuin kaupallisetkin tahot. Työn jälkimmäisessä osassa tarkastellaan näitä ilmiöitä ja niiden vaikutusta yksityisen henkilön elämään. Tutkielmassa käsitellään myös niin kutsuttuja sähköisiä jalanjälkiä, joita voidaan joissakin tapauksissa pitää henkilötietoina. Henkilötietojen käsittely asettaa rekisterinpitäjälle vastuita ja velvollisuuksia, mutta kuka viime kädessä vastaa tietoverkkojen käytön jättämistä jäljistä ja miten niiden kanssa tulisi menetellä? Lopuksi esitellään kehitteillä olevia standardeja ja muita käytänteitä, joilla yksityisyyttä voidaan tietoverkoissa suojella.

1.3. Menetelmän ja lähteiden kuvaus

Tutkielma perustuu suurimmaksi osaksi kirjallisen aineiston läpikäymiseen. Kirjallisista lähteistä tärkeimpänä on käytetty suomalaisten tietosuojaviranomaisten kirjoituksia ja kannanottoja, joista pääosa on peräisin tietosuojalautakunnan ja tietosuojavaltuutetun toimiston julkaisemasta Tietosuoja-lehdestä. Lehdessä julkaistaan runsaasti myös yhteiskunnan muiden alojen asiantuntijoiden kirjoituksia viranomaiskannanottojen lisäksi. Tietosuoja-lehden vuosikerrat on käyty tutkielmaa varten läpi vuodesta 1996 alkaen.

Tietosuojalainsäädäntöä ja periaatteita käsittelevän osuuden parhaita lähteitä ovat puolestaan olleet lainsäätäjän esivalmistelutyöt, joista löytyvät aikanaan tehtyjen ratkaisujen perustelut ja tietosuojan linjaukset. Painettujen julkaisujen lisäksi muun muassa uusimmat hallituksen esitykset ovat saatavissa myös Finlex-säädöskokoelmasta[1]. Muutoin tietosuojaa ja siihen liittyvää lainsäädäntöä kommentoivaa kirjallisuutta ei sitten 1990-luvun alkupuolen ole paljoakaan julkaistu. Tärkeimmät kommentaariteokset ovat jo vuosilta 1991 ja 1992 — toisaalta useimmat henkilötietojen käsittelyn pääperiaatteista eivät toistaiseksi ole näistä ajoista miksikään muuttuneet.

Aihetta valaisevia esimerkkiaineistoja on enimmäkseen saatu Tietosuoja-lehdestä ja verkkosivuilla julkaistuista tietosuojavaltuutetun kannanotoista. Tutkielmaa varten on käyty läpi myös kaikki tietosuojalautakunnan päätökset Finlex-tietokannasta. Säädöskokoelmassa ei kuitenkaan ollut montakaan Internetiin liittyvää ratkaisua, eivätkä löytyneet esimerkit sopineet tutkielman aihepiiriin.

Tietosuojavaltuutetun toimisto luonnollisestikin julkaisee tutkielman aiheeseen liittyvää ohjeistusta, jota on saatavilla myös toimiston www-sivuilta[2]. Muita Internetistä löytyneitä aineistoja edustavat lähinnä yksityisyyttä tukevien teknologioiden lähteet, jotka ovat peräisin W3C-konsortion (*World Wide Web Consortion, W3C*) verkkosivuilta. Muutoin verkosta on löytynyt joitakin aineistona käytettyjä yksittäisiä esimerkkejä.

[1] http://www.finlex.fi
[2] http://www.tietosuoja.fi

Tutkielmassa esitellyt www-sivut puolestaan edustavat tavanomaisia Internet-palveluita, jotka on poimittu mukaan satunnaisin perustein.

2. Oikeus yksityisyyteen

Suomessa yksityisyyden suoja on perusoikeus, josta säädetään hallitusmuodon toisessa luvussa. Perustuslain 10. §:n pykälän mukaan: "Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla." Pykälässä mainittu henkilötietojen suoja on taattu tietosuojalainsäädäntöön kuuluvalla henkilötietolailla.

Yksityisyydestä tuli perusoikeus hallitusmuodon uudistuksen yhteydessä vuonna 1995. Perusoikeusuudistuksen taustalla oli perusoikeuksien laajentaminen ja täsmentäminen kansainvälisten ihmisoikeussopimusten mukaisiksi. [Mahkonen, 1997]

2.1. Yksityisyyden määrittely

Vaikka tietosuojalainsäädännön esitöissä on käsitelty yksityisyyttä, on tämä käsite tarkoituksellisesti jätetty määrittelemättä [HE 49/1986; HE 96/1998]. Yksityisyyden täsmällinen määrittely vaikuttaa olevan hankalaa ellei jopa mahdotonta [Konstari, 1992; Saarenpää, 2004]. Toisinaan puhutaan myös yksityiselämästä, vaikka sitä tarkalleen ottaen ei voi pitää yksityisyyden synonyyminä [Mahkonen, 1997].

Saarenpään [2004] mukaan täsmällisten määritelmien löytäminen on vaikeaa ajatuksellisille asioille. Kyse on pikemminkin suhdekäsitteestä, jossa yksityisyys rajautuu suhteessa valtioon, yhteiskuntaan, ihmiskäsitykseen ja teknologiaan. Wallinin ja Nurmen [1991] mukaan yksityisyyden käsite saa merkityksensä ja sisältönsä muun muassa aika-, arvostus- ja yhteiskuntasidonnaisesti. Mahkonen [1997] lisää tähän luetteloon vielä näkökulma-, käsite-, laki- ja kulttuurisidonnaisuuden. Siinä missä mikään muu taho ei määrittele kunnolla yksityisyyttä edes tietyssä asiayhteydessä, Mahkonen [1997] uskaltautuu sentään antamaan käsitteelle seuraavia merkityksiä:

— fyysinen ja psyykkinen koskemattomuus
— arvokkuuden tunteen säilyttäminen
— itsemääräämistä turvaava riippumattomuus
— itseään koskevan tiedon kontrollointi
— mahdollisuus torjua sivullisten tunkeutuminen omaan elämään
— luottamuksellisuuden taustalla oleva perusarvo.

2.2. Yksityisyys ja tietosuoja

Yksityisyys ja tietosuoja liittyvät läheisesti toisiinsa, ja riippuu tarkastelunäkökulmasta, kumpaa käsitteistä pidetään yläkäsitteenä. Mahkosen [1997] mukaan yksityisyyden suojan katsotaan muodostuvan persoonallisuuden suojasta, intimiteettisuojasta ja tietosuojasta, kun lainsäätäjä puolestaan tietosuojalainsäädännön esitöissä on käsitellyt yksityisyyden suojaa tietosuojan osana.

Tietosuojalainsäädännön perustuksia luotaessa 1980-luvulla tietosuojaan on katsottu kuuluvan

— kansalaisten yksityisyyden suojan ja oikeusturvan huomioon ottaminen rekisteröinnissä
— tiedostojen suojaaminen luvattomalta ulkopuoliselta käytöltä sekä
— valtion turvallisuuden ja yhteiskunnan avoimuuden varmistaminen rekisterinpidossa [HE 49/1986].

Tietosuojan tarkoitukseksi on määritelty tiedon kohteena olevan henkilön etujen, oikeuksien ja yksityisyyden turvaaminen [HE 96/1998]. Tietosuojan keskeisenä tarkoituksena nähdään myös rekisteröidyn ja rekisterinpitäjän suhteen avoimuuden lisääminen [Aarnio, 2003]. Tietosuojasäännösten tehtäväksi on puolestaan annettu ratkaisumallien osoittaminen yksityisyyden suojan ja tiedontarpeiden välisissä ristiriitatilanteissa. Tämä on osa yhteiskunnan toimivuuden turvaamista. [HE 49/1986]

Saarenpään [1992; 1994] mukaan tietosuojasta puhuminen on harhaanjohtavaa, sillä suojaa eivät saa niinkään tiedot vaan yksityinen henkilö. Koska suojattava taho, yksityinen luonnollinen henkilö, ei ilmene tietosuojan käsitteestä, aiheuttaa se jopa kielteisiä mielleyhtymiä. Tietosuoja ei sisällä ilmaisuna samanlaista myönteistä sanomaa, kuten esimerkiksi tekijänoikeus.

Yksityisyyden suojaa arvioitaessa on muistettava, ettei tarkoituksena ole ensisijaisesti toimia yksittäisten vaatimusten mukaan. Kyse on paremminkin tietyn yksityisyyden suojan tason saavuttamisesta tai tietojenkäsittelyn laillisuuden yleisistä edellytyksistä. [Partanen, 1996] Pääasia onkin, ettei tietosuojaa sinänsä ryhdytä pitämään jonakin itseisarvona. Tietosuojan tulee pikemminkin olla väline muiden arvojen saavuttamiseksi. Sitä paitsi tietosuojaakin voidaan rajoittaa, mikäli muut, tärkeämmät edut niin vaativat. [Heinonen, 1994]

2.3. Yksityisyys oikeuksien kokonaisuutena

Tietosuojalainsäädännön valmistelutöissä yksityisyyttä on käsitelty toiminnallisesti, rekisterinpitäjälle syntyvinä velvoitteina, ja toisaalta kansalaisille syntyvinä oikeuksina. Lainsäätäjä on määritellyt yksityisyyden suojan keskeisimmiksi osiksi seuraavat oikeudet: 1) oikeus tietää ja päättää itseään koskevien tietojen käytöstä 2) oikeus järjestää elämänsä ilman perusteetonta ulkopuolisten puuttumista ja 3) oikeus muutenkin vapaasti päättää itseään koskevista asioista lainsäädännön rajoissa. [HE 49/1986]

Aarnion [2003] mukaan yksityisyyttä onkin helpompi arvioida, kun käsitellään oikeutta yksityisyyteen, vaikka Mahkonen [1997] tällaista käsitteiden välineellistämistä arvosteleekin. Henkilötietojen käsittelyssä Aarnio [2003] on koonnut yksityisyyden suojaan seuraavat oikeudet:

Oikeus tietää tietojensa käsittelystä; kuka kerää, tallettaa ja käyttää rekisteröityä koskevia tietoja ja mihin tarkoitukseen. Rekisterinpitäjälle on asetettu aktiivinen informointivelvoite [HE 96/1998]. Kansalaisilla on myös oikeus tietää niiden rekistereiden olemassa olosta, joihin heistä tietoja kerätään [HE 49/1986].

Henkilötietojen käsittelyn on aina oltava perusteltua [Aarnio, 2003]. Rekisteröidyllä on oikeus tutustua itseään koskeviin tietoihin, vaikka ne olisivat salassa pidettäviä. Henkilötietolaissa tämä on ilmaistu rekisteröidyn tarkastusoikeutena.

Oikeus päättää itseään koskevien tietojen käsittelystä. Yksityiselämää koskevien tietojen kerääminen ja käyttö on ilman rekisteröidyn suostumusta rajoitettava vain välttämättömimpään [HE 49/1986]. Saarenpää [2004] korostaa, että yksityisyyteen kuuluva oikeus anonymiteettiin koskee sekä julkisia että yksityisiä rekisterinpitäjiä. Henkilötietojen käsittelyn perusedellytykseen, informoituun suostumukseen (*informed consent*), kuuluu olennaisesti se, että henkilö saa riittävästi tietoa päätöksentekonsa tueksi [Aarnio, 2003]. Henkilön tulee siis tietää, mihin hän suostuu. Ilmaisu informoitu suostumus on levinnyt terveydenhuollon yhteydestä muuhunkin rekisterinpitoon [Mahkonen, 1997].

Henkilötietolaissa suostumuksella tarkoitetaan vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua. Mikäli suostumuksen olemassaolosta syntyy kiistaa, todistustaakka suostumuksesta on rekisterinpitäjällä. Lisäksi henkilöllä on oikeus peruuttaa suostumuksensa milloin tahansa. [HE 96/1998]

Oikeus järjestää yksityiselämänsä ilman perusteetonta ulkopuolisten puuttumista. Tällaista puuttumista on esimerkiksi taloudellisissa tai yhteiskunnallisissa kysymyksissä tehtäviin päätöksiin vaikuttaminen. Perusteetonta puuttumista on myös kansalaisen tietämättä toteutettu valvonta. [HE 49/1986]

Oikeus tulla arvioiduksi virheettömien ja tarpeellisten tietojen perusteella. Rekisterinpitäjä velvoitetaan aktiivisesti ylläpitämään rekistereitään [Aarnio, 2003]. Henkilötietolaissa säädetään, että rekisterinpitäjän on rekisteröidyn vaatimuksen lisäksi myös oma-aloitteisesti oikaistava tai poistettava rekisterissä oleva virheellinen, tarpeeton tai vanhentunut tieto.

Tietojen tarpeellisuutta arvioitaessa rekisterinpitäjän yksinomainen arvio ei riitä [HE 49/1986]. Tarpeellisuuden tulee sen sijaan olla objektiivisesti havaittavaa [Aarnio, 2003]. Henkilötietoja pidetään tarpeellisina, kun ne ovat asianmukaisia ja olennaisia. Tiedot eivät myöskään saa olla liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään. [HE 96/1998]

Oikeus voida luottaa tietoturvallisuuden riittävään tasoon. Rekisterinpitäjälle on asetettu tietoturvallisuusvelvoite: henkilötietojen käsittely on suojattava luvattomalta käyttämiseltä, muuttamiselta ja tuhoamiselta, eivätkä sivulliset saa päästä henkilötietoihin käsiksi [Aarnio, 2003]. Rekisterinpitäjän on määriteltävä tietojen käyttöoikeudet ja varmistettava oikeutettu tietojen käsittely esimerkiksi salasanajärjestelmällä. Rekisteri on myös suojattava laittomilta käsittelyn yrityksiltä. Lisäksi tietojen siirtäminen on varmistettava siten, että siirto ei aiheuta tiedoissa muutoksia. [HE 96/1998]

Oikeus saada viranomaisilta apua. Riittävä yksilön suoja on turvattava lailla, ja valtion on huolehdittava myös valvontaviranomaisen olemassaolosta [Aarnio, 2003].

Lisäksi henkilötietolaissa on rekisteröidyn oikeuksiksi nimetyssä kuudennessa luvussa säännös **kielto-oikeudesta**. Rekisteröidyllä on oikeus kieltää tietojensa käsittely suoramainontaa ja -markkinointia, markkina- ja mielipidetutkimusta sekä henkilömatrikkelia ja sukututkimusta varten.

2.4. Miksi yksityisyyttä on tietojenkäsittelyssä suojeltava?

Tietosuojan tarve on tullut ilmeiseksi tietokoneiden käytön yleistymisen myötä. Tietotekniikalla voidaan hallita suuria tietomääriä sekä yhdistellä ja etsiä tietoja tehokkaasti. Alan nopea kehitys mahdollistaa yhä laajempien tietomäärien käsittelyn entistä halvemmalla. Kansalaisia koskevien tietojen kerääminen, käyttö ja yhdistely luo mahdollisuudet yksityiselämän valvontaan. Sääntelemättömänä rekisteröintitoiminnan on katsottu sisältävän riskin kontrolloimattoman vallankäytön synnystä. [HE 49/1986]

Yksityisyyden suojan loukkauksia ei ole lainsäädännössä eritelty. Yleisesti voidaan todeta, että yksityisyys vaarantuu, mikäli tietosuojalainsäädännön periaatteita ei noudateta. Vastaavasti yksityisyyden suojan loukkauksena henkilötietoja käsiteltäessä pidetään tietosuojalainsäädännön vastaista menettelyä. [Partanen, 1995; 1996]

Esimerkiksi tietojen yhdistely on aina altista erehdyksille ja virheille, mutta erityisesti eri organisaatioiden erilaisista tietolähteistä peräisin olevan tiedon yhdistäminen voi vaarantaa yksityisyyden. Heinonen [2001a] on listannut ongelmia aiheuttaviksi seikoiksi seuraavia esimerkkejä:

— tietolähteet ovat vajavaisia
— tiedon sisällön lisäksi myös sen merkitys voi olla virheellinen
— tiedon merkitystä ei tunneta
— tiedon laatu on huono tai puutteellinen
— yhdistelyprosessi on puutteellinen ja tuloksena saadaan huonolaatuista tietoa
— tiedon ja sen kohteen välillä ei ole yhteyttä tai se on vaillinainen
— saatua yhdistelmätietoa käytetään syrjivästi, loukkaavasti tai muutoin asiattomasti.

Tiedon yhdistelyssä yksittäisten tietolähteiden virheellisyydet saattavat moninkertaistua. Vaikka samasta tietolähteestä johdetut tiedot eivät välttämättä ole yhdistelemällä saatuja luotettavampia, ovat ne yleensä johdonmukaisempia. [Heinonen, 2001a] Tietosuojalainsäädännössä onkin säännelty rekisterinpitäjän tiedonsaantioikeutta tietojen suunnittelu- ja käyttötarkoitussidonnaisuuden periaatteilla. Partanen [1995] perustelee rajoituksia seuraavasti: mikäli tiedon saantioikeudet olisivat laajat ja vastaavasti tiedon tarpeet epämääräisiä, voitaisiin helposti hankkia tietoa, joka ei olisi sisällöllisesti yhteensopivaa vertailtavan tai muutoin jo käytössä olevan tiedon kanssa. Tällöin tietojen saanti saattaisi johtaa jopa virheelliseen lopputulokseen.

Tieto voi siis oikeasta asiayhteydestä irrotettuna johtaa epäluotettavaan ja väärään arviointiin — esimerkiksi ansiotulon käsite on erilainen eri yhteyksissä [Partanen, 1995]. Muun muassa verotuksen ja yrittäjän eläkemaksujen perustana käytetyt tulot voivat olla samalla henkilöllä eri suuruisia. Heinonen [2001a] korostaakin yhdistelemäl-

lä saatavan tiedon laadun kontrollointia. Kontrollilla Heinonen tarkoittaa eri tietolähteiden vertailtavuuden ja niiden sisältämien tietojen laadullisen yhdenmukaisuuden varmistamista.

Korpelan [2003a] mielestä yksi keskeisimmistä yksityisyyden uhista on datan keruun teknologinen imperatiivi, jonka mukaan kaikki tallennettavissa oleva tieto pitää tallentaa. Tietojärjestelmien suunnittelijoiden periaatteena on kerätä tietoja varmuuden vuoksi, koska niiden saanti olisi jälkikäteen hankalaa, ellei mahdotonta. Tietojen tarpeellisuutta ei arvioida, sillä tarpeen ajatellaan voivan syntyä vasta myöhemmin. Lisäksi tietojen turhaa keräämistä vähätellään vaikkapa sillä, ettei tietoja käytetä. Korpela kuitenkin korostaa, että tietoturvassa on aina aukkoja. Mikäli jossakin on tietoa, sillä on mahdollisuus päätyä sivullisille rikoksen tai silkan huolimattomuuden vuoksi. Tiedot voivat joutua vääriin käsiin myös vahingossa. Esimerkiksi potilastietoja on löytynyt niin kaatopaikoilta kuin käytöstä poistettujen tietokoneitten kovalevyiltäkin. Näin ollen riskien minimoimiseksi on perusteltua vaatia henkilötietojen keräämisen sääntelyä ja rajaamista vain välttämättömimpään. Korpela katsookin, että yksi käytännöllisimpiä perusteluja yksityisyyden suojalle on tilastollinen varmuus siitä, että salassa pidettäviä tietoja vuotaa. [Korpela, 2003a; 2003b]

Korpela [2003b] painottaa myös, että yksityisyyttä ja henkilötietoja on suojattava järjestelmällistä hyväksikäyttöä vastaan. Kyse on varautumisesta laillisuuden rajoilla olevaan toimintaan, suoranaisiin rikoksiin tai sellaisiin yhteiskunnallisiin muutoksiin, joista ei välttämättä nyt ole näkyvissä ennusmerkkejä. Korpelan mielestä on realistista olettaa odottamattomien asioiden tapahtumista.

Tietosuojalainsäädäntö on lainsäätäjän kannanotto tietojärjestelmien mukanaan tuomiin riskeihin yksityisen henkilön kannalta [Partanen, 1995]. Lain tarkoituksena on ehkäistä jo ennalta yksityisyyden suojaan kohdistuvat loukkaukset [HE 49/1986]. Yksityisyyden suojaus koostuu kuitenkin kahdesta osasta: mikäli yksityisyys on tullut loukatuksi, järjestelmän jälkikäteen toimivana osuutena sovelletaan rikosoikeudellisia sanktioita [Aarnio, 2003].

2.5. Yksityisyyden oikeuden rajoituksia

Oikeus yksityisyyteen ei ole ehdoton. Perustuslain tasolla säädetään myös julkisuusperiaatteesta, jonka mukaan kansalaisilla on oikeus saada tietoja viranomaisten asiakirjoista [PeL 12 §]. Julkisuusperiaatettakin voidaan silti erikseen rajoittaa esimerkiksi salassapitosäännösten nojalla.

Perusoikeudet eivät saa olla keskenään ristiriidassa. Niinpä yksityiselämän suojan ja tiedon saamisoikeuden välistä suhdetta on mietittävä tilannekohtaisesti. Mikäli yksittäistapauksissa syntyy vastakkaisten oikeusohjeiden ristiriita, on se ratkaistava vakiintuneiden tulkintaperiaatteiden mukaisesti. Vakiintunut käytäntö muodostuu oikeuden ennakkopäätösten myötä. Lisäksi lainvalmistelutöissä otetaan kantaa siihen, miten säännöksiä

arvioidaan sekä yksityisyyden ja tiedonsaannin oikeuksia rajoitetaan. [Mahkonen, 1997; Wallin, 1998]

Perusoikeuksiin vedottaessa on pidettävä mielessä perimmäinen tarkoitus, joka kunkin oikeuden taustalla on. Julkisuusperiaatteella edesautetaan osallistumista yhteisten asioitten hoitoon ja valvotaan julkista vallankäyttöä. Periaatetta ei siis tule käyttää yleisenä tiedonhankintakeinona toisten yksityisasioista. [Wallin, 1998] Sama koskee perustuslain 12. §:ssä säädettyä sananvapautta. Korpela [2003a] huomauttaa, että useimmiten kyse on vain kaupallistetusta juoruamisesta, kun yksityisasioita haluttaisiin sananvapauden nimissä levitellä.

Tietosuojalainsäädännössä on turvattu yhteiskunnallisesti merkittävän tiedon saatavuus tieteellistä tutkimusta, tilastointia sekä viranomaisen suunnittelu- ja selvitystehtäviä koskevin poikkeussäännöksin [HetiL 14 §, 15 § ja 16 §]. Näiden lisäksi tiedonsaantioikeutta tarvitaan muun muassa vastuusuhteiden selvittämiseen. Yksityisyyden nojalla ei saa pimittää tietoa siitä, kuka käyttää yrityksissä omistaja- tai päätöksentekovaltaa. Myös taloudelliseen tai poliittiseen valtaan perustuvien menettelyjen on oltava yleisesti tiedossa. Yksilön asema ja rooli vaikuttavat näin itseä koskevien tietojen määräämisvaltaan. [Wallin, 1998] Lisäksi eri osapuolten välinen suhde ja henkilötietojen käyttöyhteys saattavat asettaa rekisteröidylle alistumisvelvollisuuden [HE 96/1998]. Esimerkiksi viranomaistoiminnassa tietoja hankitaan jopa rangaistuksen uhalla tehostetuin ilmoitusvelvollisuuksin. Oikeus yksityisyyteen on siis väistämättä suhteellista, ja kansalaisilla on oikeus päättää tietojensa käytöstä, ellei laissa toisin säädetä.

3. Tietosuojalainsäädäntö

Toisinaan saatetaan puhua harhaanjohtavasti tietosuojalaista, vaikka sen nimistä lakia ei Suomessa ole [Korpela, 2003b]. Sen sijaan voidaan puhua tietosuojalainsäädännöstä. Tämän tutkielman aihepiirin kannalta tärkeimmät tietosuojalainsäädäntöön kuuluvat yleislait ja sopimukset ovat

— 1.1.1988 voimaan tullut, sittemmin kumottu henkilörekisterilaki
— Euroopan neuvoston vuonna 1981 hyväksymä yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, joka tuli Suomen osalta voimaan 1992
— Euroopan yhteisöjen vuonna 1995 antama henkilötietodirektiivi, joka tuli jäsenmaiden implementoitavaksi vuonna 1998
— 1.6.1999 voimaan astunut henkilötietolaki, joka korvasi henkilörekisterilain.

Henkilötietodirektiivin virallinen nimi on Euroopan Unionin direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta [95/46/EY]. Direktiivin virallisen nimen pituudesta johtuen jäljempänä tutkielmassa käytetään lyhennettyä nimitystä henkilötietodirektiivi. Tutkielman vanhemmissa lähteissä henkilötietodirektiivistä tosin käytetään nimitystä tietosuojadirektiivi, mutta tietosuojaan liittyvien direktiivien lisäännyttyä nimitystä on tarkennettu.

Henkilötietolaki on henkilötietojen käsittelyä koskeva yleislaki, jota sovelletaan, ellei muualla laissa toisin säädetä [HetiL 2 §]. Eduskunnan hallintovaliokunta on todennut, ettei henkilötietolaki tule ratkaisemaan kaikkia henkilötietojen käsittelyyn eri aloilla liittyviä yksittäisiä kysymyksiä. Sen vuoksi tarvitaan toimialakohtaista erityislainsäädäntöä. [HaVM 26/1998] Tutkielman kannalta tärkeimpiä henkilötietolakia täydentäviä erityislakeja ovat

— sähköisen viestinnän tietosuojadirektiivi [2002/58/EY], joka annettiin 12.7.2002, ja
— sähköisen viestinnän tietosuojalaki, joka astui voimaan 1.9.2004.

3.1. Tietosuojalainsäädännön kehitys

Suomessa henkilötietojen käsittelystä on säädetty lailla 1.1.1988 alkaen, jolloin henkilörekisterilaki astui voimaan. Kansainvälisesti vertailtuna laki saatiin aikaan melko myöhään, sillä useissa länsimaissa vastaavat säännökset oli säädetty jo 1970-luvulla [HE 49/1986]. Ennen henkilörekisterilain voimaan tuloa lainsäädännössä ei ollut yhtenäisiä säännöksiä yksityisyyden suojasta eikä henkilörekistereiden pitämisestä. Henkilötietoja sai kerätä ja tallentaa lähes rajoituksetta. Myös henkilötietojen yhdistely ja luovuttaminen oli puutteellisesti säänneltyä. Kansalaisilla ei ollut mahdollisuutta valvoa heitä itseään koskevien tietojen käyttöä — useimmiten henkilörekistereiden olemassaolo ja käyttö ei ollut edes tiedossa. Tietojen oikeellisuutta ei tietoja tallennettaessa aina tarkistettu. [HE 49/1986]

Henkilörekisterilaista tuli aikanaan osa tietosuojalainsäädännöksi nimitettävää kokonaisuutta. Lailla vahvistettiin ne periaatteet, joita henkilötietojen käsittelyssä tulee yleisesti noudattaa. Nämä 1980-luvulla mietityt tietosuojaperiaatteet ovat yhä voimassa. Kun henkilörekisterilain voimaantulosta oli kulunut kymmenen vuotta, kaipasi lainsäädäntö teknisen ja yhteiskunnallisen kehityksen vaatimaa ajanmukaistamista. Tärkeimpänä henkilörekisterilain uudistamisen pontimena olivat kuitenkin Suomen perustusoikeusuudistuksen vaatimat muutokset ja kansallisen lainsäädännön saattaminen EU:n henkilötietodirektiivin tasolle. [HE 96/1998] Perusoikeusuudistuksen johdosta henkilötietojen käsittelyn säätelytasoa oli nostettava. Osa henkilötietojen käsittelyn keskeisistä säännöistä oli säädetty lakia alemmalla tasolla, henkilörekisteriasetuksessa. Perusoikeuksiin mukaan otetun Yksityiselämän suoja -pykälän sanamuotona on: "Henkilötietojen suojasta säädetään *lailla*." Lisäksi yksityisyyden suoja tuli sopeuttaa yhteen julkisuuslainsäädännön kanssa.

Yhtäältä EU:n ja toisaalta informaatioteknologian kehityksen myötä Suomessa jouduttiin lain uudistuksen yhteydessä irtautumaan rekisterikäsitteestä. Henkilörekisterilain aikana vallitsi tiedon elinkaariajattelu, jossa on eroteltu henkilötietojen käsittelyn eri vaiheet: kerääminen, tallentaminen, käyttö, luovutus, arkistointi ja hävittäminen. Direktiivissä puolestaan puhutaan yleisesti henkilötietojen käsittelystä (*processing of personal data*), joka sisältää kaikki henkilötietoihin kohdistuvat toiminnot. [HE 96/1998; Konstari, 1997] Uuden henkilötietolain säännöksissä ei siis edellytetä, että atk:n avulla käsiteltävien henkilötietojen tulisi nimenomaisesti muodostaa henkilörekisteri, jotta toiminta kuuluisi lain soveltamisalaan [HE 96/1998].

Henkilörekisterilakia säädettäessä henkilötietojen keruuta haluttiin rajoittaa myös valtion turvallisuuden vuoksi [HE 49/1986]. Vielä 1970- ja 1980-luvuilla massiivista tietojen kokoamista tietojärjestelmiin pidettiin uhkakuvana — olisivathan tällaiset keskitetyt ja kattavat rekisterit mitä otollisinta tietoa, mikäli vieras valta miehittäisi Suomen [Korpela 2003b]. Valtion turvallisuudesta huolehtiminen on sittemmin väistynyt informaatioteknologian kehityksen myötä. Tietojenkäsittely on pikemminkin hajautunut, eikä suuren supertietopankin syntyminen ole enää todennäköinen kehityssuunta. [Konstari, 1997] Lisäksi henkilörekisterilain uudistustyössä lainsäätäjä halusi erityisesti korostaa lain keskeistä tavoitetta, yksityisyyden suojaa. Niinpä henkilötietolain ensimmäisestä pykälästä jätettiin tarkoituksella pois maininta valtion turvallisuudesta, vaikka se lain yksittäisissä säännöksissä vielä mainitaankin. [HE 96/1998]

Henkilörekisterilain muuttamisessa oli aluksi tarkoitus selvitä pienehköin tarkistuksin ja osittaisuudistuksella. Säädöstekstin selvyyden vuoksi laki päätettiin lopulta kirjoittaa kokonaan uudelleen. [HE 96/1998] Konstarin [1997] mukaan ratkaisuun vaikutti myös direktiiviuskollisuus. Henkilörekisterilaki siis kumottiin ja sen tilalle astui voimaan henkilötietolaki.

Tutkielman aihepiirin kuuluva erityislaki — sähköisen viestinnän tietosuojalaki — puolestaan kumosi viitisen vuotta voimassa olleen lain yksityisyyden suojasta televies-

tinnässä ja teletoiminnan tietoturvasta. Partasen [2004] mukaan alunperin teletoiminnan säännöksiä on vähitellen laajennettu koskemaan yleisemminkin sähköisen viestinnän eri osapuolia. Uusi sähköisen viestinnän tietosuojalaki ja erityisesti siihen kuuluva pykälä evästeiden (*cookies*) käsittelystä siis velvoittaa tutkielmassa käsiteltävien verkkopalvelusivustojen tarjoajia.

3.2. EU:n vaikutus Suomen tietosuojalainsäädäntöön

Vuonna 1995 hyväksytty henkilötietodirektiivi astui voimaan 24.10.1998, jolloin jäsenmaiden tuli se implementoida. Implementoinnilla tarkoitetaan kansallisen lainsäädännön saattamista direktiivin mukaiseksi. Suomessa "Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi HE 96/98" oli direktiivin implementointihetkellä parhaillaan eduskuntakäsittelyssä, joten Suomessa ei täysin pysytty tavoiteaikataulussa.

Henkilötietodirektiivin tavoitteena on turvata yksilöiden perusoikeudet ja -vapaudet ja erityisesti oikeus yksityisyyteen henkilötietojen käsittelyssä. Direktiivi liittyy Euroopan yhteisön sisämarkkinoiden kehittämiseen ja sen toisena päätavoitteena on henkilötietojen vapaa liikkuminen EU:n jäsenvaltioiden välillä. [HE 96/1998] Direktiivi määrittelee eurooppalaisen tietosuojan vähimmäistason, joka voidaan toki kansallisella lainsäädännöllä ylittää. Esteetön ja luotettava henkilötietojen siirto jäsenmaasta toiseen edellyttää yhteisesti hyväksyttyä tietosuojalainsäädännön tasoa ja lakien valvontaa [Kuopus, 1996].

Suomalainen lainsäädäntö vastasi jo henkilörekisterilain voimassa ollessa varsin hyvin eurooppalaista tietosuojan tasoa. Lainsäännökset oli aikanaan valmisteltu ottamalla huomioon Euroopan neuvoston jäsenvaltioiden vuonna 1981 tekemä tietosuojasopimus. Henkilötietodirektiivi kuitenkin täsmensi sen pohjana ollutta tietosuojasopimusta, joten direktiivin vaatimukset osittain poikkesivat henkilörekisterilain säännöksistä. [HE 96/1998]

Yksi olennaisimmista EU:n mukanaan tuomista muutoksista on henkilötietolain soveltamisalan laajeneminen aiempaan henkilörekisterilakiin nähden. Ensinnäkin lakia sovelletaan kaikkiin henkilötietojen käsittelyvaiheisiin: keräämiseen, tallentamiseen, järjestämiseen, käyttöön, siirtämiseen, luovuttamiseen, säilyttämiseen, muuttamiseen, yhdistämiseen, suojaamiseen, poistamiseen, tuhoamiseen ja muihin henkilötietoihin kohdistuviin toimenpiteisiin. Toiseksi lain soveltamisala laajeni lähtökohtaisesti kaikkiin luonnollisiin henkilöihin, kun henkilörekisterilaki koski vain yksityisiä henkilöitä. [Henkilötietojen käsittelyä.., 1999] Suomessa on perinteisesti ajateltu, että esimerkiksi virkaa hoitava henkilö ei tarvitse yksityisyyden suojaa julkista asemaansa koskevien henkilötietojen osalta. Henkilötietolaissa säädetäänkin edelleen oikeudesta erikseen käsitellä henkilön asemaa, tehtäviä, niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavia tietoja, jotka ovat yleisesti saatavilla. Tietojen käsittelyn on kuitenkin johdut-

tava rekisterinpitäjän tai tiedot saavan oikeuksien turvaamisesta. [HetiL, 8 § 1 mom. 8 kohta]

Henkilötietodirektiivi lisäsi rekisteröityjen tiedonsaantioikeuksia entisestään, sillä lakiin on kirjattu nimenomainen rekisteröityjen informointivelvoite. Rekisterinpitäjän tulee antaa tiedot rekisteröitävien henkilötietojen käsittelyyn liittyvistä seikoista viimeistään henkilötietoja kerättäessä. Rekisterinpitäjän laatimaa rekisteriselostetta koskeva velvoite laajeni siten, että selosteessa tulee nykyisin olla myös kuvaus rekisterien suojauksen periaatteista. Kuvaus ei tosin saa olla liian tarkka, sillä yksityiskohtaiset suojaustiedot on pidettävä ulkopuolisilta salassa. Henkilötietoja koskevan virheen oikaisussa rekisteröidyn ei tarvitse enää perustella, miksi hän pyytää oikaisua. Rekisterinpitäjällä on myös velvollisuus estää virheellisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn oikeuksia. [Henkilötietojen käsittelyä..., 1999]

Myös valvontajärjestelmä muuttui uuden lain myötä. Merkittävimpänä muutoksena lakiin tuli uusi pykälä toimialakohtaisten käytännesääntöjen laatimisesta. Käytännesääntöjen tavoitteena on antaa ohjeita nimenomaisilla toimialoilla — esimerkiksi atk-alalla — henkilötietojen käsittelyn erityiskysymyksissä. Hajautetun tietojenkäsittelyn kannalta tärkeä uudistus on rekisterinpidon vastuiden jakamismahdollisuus. Henkilörekisterillä voi nykyisin olla useampikin kuin yksi rekisterinpitäjä. Useamman eri rekisterinpitäjän rekistereitä ei silti edelleenkään saa yhdistää vastoin lain säännöksiä. [Henkilötietojen käsittelyä..., 1999]

3.3. Tietosuojalainsäädännön erityiset tavoitteet

Henkilörekisterilain tarkoituksena oli parantaa tietosuojan tasoa Suomessa. Lain erityisenä, toiminnallisena tavoitteena oli saada aikaan yhtenäinen ja hyvä rekisteritapa. Henkilörekistereiden käyttö haluttiin yhtenäistää siten, että kansalaiset voisivat luottaa rekisteritoimintaan. [HE 49/1986] Nykyisessä henkilötietolaissa lain tarkoitukseksi on määritelty yksityiselämän suojan ja muiden yksityisyyden suojaa turvaavien perusoikeuksien toteuttaminen. Lailla turvataan se, ettei yksityisyyden suojaa rajoiteta ilman laissa säädettyä perustetta. Hyvä rekisteritapa on ajanmukaistettu tavoitteeksi edistää hyvään tietojenkäsittelytapaan perustuvaa yhtenäistä käytäntöä henkilötietojen käsittelyssä. [HetiL 1 §; HE 96/1998]

Henkilörekisteri- ja henkilötietolain pyrkimyksenä on, että rekisterinpitäjä toimisi tietosuojan parantamiseksi oma-aloitteisesti. Lainsäätäjä on näin korostanut rekisterinpitäjän itseohjautuvuutta ja tämä tavoite on käytännesääntöjen myötä painottunut entisestään. Tietosuojalainsäädännön erityistavoitteena on myös yhteiskunnan tiedollisten vaatimusten turvaaminen. Tämä tarkoittaa tarvittavien henkilötietojen saatavuuden turvaamista sekä määrällisesti että laadullisesti. Laadulla tarkoitetaan tietojen oikeellisuutta, ajantasaisuutta ja luotettavuutta. Partanen [1995] nimittää tietosuojalainsäädännöllä tavoiteltavaa luotettavien ja ajan tasalla olevien henkilötietojen käsittelyä yhteiseksi hyväksi.

Mistä luotettavat ja ajan tasalla olevat tiedot sitten hankitaan? Tavallisimmin ne saadaan — tai ainakin tulisi saada — henkilöltä itseltään. Jotta henkilö antaisi tiedot, on hänen voitava luottaa rekisterinpitäjään. Luottamus puolestaan saavutetaan henkilötietojen käsittelyn avoimuuden periaatteen kautta. [Partanen, 1995] Käytäntöä, jossa kansalaista koskevat tiedot saadaan lähtökohtaisesti häneltä itseltään tai vähintään hänen tietensä, nimitetään tiedolliseksi itsemääräämisvallaksi. Partanen [1995] huomauttaa, että demokraattisessa yhteiskunnassa henkilötietoja ei voida ylläpitää täysin henkilöstä irrallaan.

Sähköisen viestinnän tietosuojalain tarkoitus puolestaan on

— turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen
— edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. [SVTSL 1 §]

Sähköisen viestinnän tietosuojalain valmistelutöissä on todettu, että sähköisten viestintäpalvelujen käytössä on yksityisyyden suojaan kuuluvia ongelmia. Lainsäätäjä on tosin huomannut, ettei kaikkia ongelmia ehkä ole mahdollista poistaa kokonaan lainsäädäntöteitse, mutta ainakin ongelmien aiheuttamaa haittaa voidaan rajoittaa — esimerkki tällaisesta haitasta on sähköpostitse välitettävä, ei-toivottu suoramarkkinointi. Sähköisiä viestintäpalveluja koskevilla säännöksillä pyritäänkin ennen kaikkea varmistamaan viestintäpalvelujen toimivuus — samalla on kuitenkin tarkoitus olla rajoittamatta uusien palvelujen kehittämistä. [HE 125/2003]

3.4. Henkilötietojen käsittelyn periaatteet

Henkilötietolain toiseen lukuun on kirjattu henkilötietojen käsittelyä koskevat yleiset periaatteet, joita nimitetään tietosuojaperiaatteiksi. Aarnion [2003] mukaan tietosuojaperiaatteet ovat osa informaatio-oikeudellista suojamekanismia. Yksityisyyden suojan loukkaantumisen ennalta ehkäisyn lisäksi periaatteiden tarkoitus on ohjata rekisterinpitäjää sen toiminnassa.

Huolellisuusvelvoite. Velvoite ilmentää niin kutsuttua itseohjautuvuuden ajatusta. Sen mukaan rekisterinpitäjien on oma-aloitteisesti huolehdittava siitä, että henkilötietojen käsittely toteutetaan ottaen huomioon yksityisyyden suojaa turvaavat säännökset ja periaatteet. Henkilötietojen käsittelyllä tarkoitetaan kaikenlaisia henkilötietoihin kohdistuvia toimintoja, mutta erityisesti asianmukaista tietojen suojaamista. [HE 96/1998]

Huolellisuusvelvoitteeksi nimetyssä pykälässä [HetiL 5 §] siis toistetaan lain tarkoitus — yksilön perusoikeuksien turvaaminen [HetiL 1 §]. Lainsäätäjä on täten halunnut korostaa lain liittymistä perusoikeuksiin ja samalla lisätä lain tavoitteiden ymmärrettävyyttä. [HE 96/1998]

Avoimuusperiaate. Laissa ei suoraan puhuta avoimuusperiaatteesta, mutta käsite on vakiintunut tietosuojaviranomaisten keskuudessa. Tietosuojalainsäädännön yhtenä tavoitteena on lisätä rekisterinpitäjän ja rekisteröidyn suhteen avoimuutta [HE 49/1986].

Henkilötietojen käsittelyn avoimuutta toteuttavat laissa mainitut rekisteriselosteen laatiminen, rekisterinpitäjän ilmoitusvelvollisuus valvoville tietosuojaviranomaisille ja rekisteröidyn tarkastusoikeus.

Avoimuuden erityisenä perusteluna rekisterinpidossa on sen tuoma mahdollisuus valvoa rekistereiden avulla tapahtuvaa vallankäyttöä [HE 49/1986]. Lainsäätäjä on katsonut, että rekisterinpidon avoimuus toteutuu parhaiten rekisteröidyn suostumukseen perustuvassa henkilötietojen käsittelyssä — suostumuksen tulisi siis olla toiminnan lähtökohtana [HE 96/1998].

Suunnitteluperiaate. Henkilötietojen käsittelyn tarkoitus tulee määritellä ennen kuin tiedot kerätään. Tarkoituksesta on puolestaan ilmettävä minkälaisten tehtävien hoitamiseksi tietoja käsitellään. Lisäksi on määriteltävä tietojen säännönmukaiset hankintalähteet ja luovutuskohteet. Käsittelyn tarkoitus voidaan määritellä uudelleen, mikäli se on tarpeen, mutta uusi tarkoituskaan ei saa olennaisesti poiketa henkilötietojen alkuperäisen käsittelyn tarkoituksesta. [HE 96/1998]

Suunnitteluperiaate edustaa rekisterinpidon yleisiä edellytyksiä. Rekisterinpitäjälle asetettu rekisteriselosteen laatimisvelvoite on osa henkilötietojen käsittelyn suunnittelua [HE 96/1998].

Käyttötarkoitussidonnaisuuden periaate. Käyttötarkoitus liittyy suunnitteluperiaatteeseen, jonka mukaan tietojen käyttötarkoitus on määriteltävä ennakolta [HE 49/1986]. Vastaavasti tietoja tulee aina käyttää vain ennen tietojen keräyksen aloittamista määriteltyyn tarkoitukseen [Aarnio, 2003]. Käyttötarkoitussidonnaisuuden ja suunnittelun periaatteilla huolehditaan osaltaan tiedon laadusta. Partanen [1995] huomauttaakin, että tietyssä tarkoituksessa kerätyt tiedot ovat virheettömiä vain tässä tarkoituksessa.

Laatuperiaatteet. Laatuperiaatteet sisältävät tietojen tarpeellisuusvaatimuksen ja virheettömyysvaatimuksen. Tarpeellisuusvaatimus kuuluu rekisterin perustamisedellytyksiin [HE 96/1998], sillä käsiteltävien henkilötietojen tulee olla käsittelyn tarkoituksen kannalta tarpeellisia. Tarpeellisuusvaatimus määrittelee siis sen, mitä tietoja rekisteriin voidaan kerätä ja tallentaa. [HE 49/1986]

Virheettömyysvaatimuksessa puolestaan asetetaan rekisterinpitäjälle velvollisuus huolehtia käsiteltävien tietojen virheettömyydestä ja asianmukaisuudesta. Asianmukaisuus kuuluu suunnitteluperiaatteen lisäksi rekisterinpidon yleisiin edellytyksiin [HE 96/1998]. Asianmukaiset tiedot eivät saa olla epätäydellisiä tai vanhentuneita. Tietojen asianmukaisuus- ja virheettömyysvaatimus edustavat yhdessä rekisteröidyn tarkastusoikeuden kanssa kansalaisten oikeusturvatakeita. [HE 49/1986]

Yhteysvaatimus. Vaatimus on tietojen tarpeellisuusvaatimuksen lisäksi toinen rekisterin perustamisedellytyksistä [HE 96/1998]. Yhteysvaatimus määrittelee, kenestä tietoja saa tallentaa. Rekisteröidyllä on oltava asiallinen yhteys rekisterinpitäjän toimintaan. Tällainen yhteys syntyy esimerkiksi asiakas- tai palvelussuhteen perusteella. [HE 49/1986]

Tietosuojaperiaatteita on arvioitava kokonaisuutena ja sovellettava yhtaikaisesti, ei yksittäin. Esimerkiksi rekisteröitävän suostumuksellakaan ei saa kerätä ja käsitellä käyttötarkoituksen kannalta tarpeettomia tietoja — suostumus ei siis poissulje tarpeellisuutta. [Aarnio, 2003]

3.5. Lakeja kohtaan osoitettu kritiikki

Henkilörekisterilaki säädettiin aikanaan tarkoituksellisesti väljiä säännöksiä sisältäväksi tietosuojan yleislaiksi. Lain pääpiirteet muotoillut tietosuojakomitea perusteli lain yleisluontoisuutta sillä, ettei henkilötietojen rekisteröinnissä sattuvia etujen ja oikeuksien loukkauksia ollut mahdollista etukäteen säännellä tyhjentävästi. Komitea oletti, että henkilörekisteröinnin ohjausta ja valvontaa varten perustettavat tietosuojaviranomaiset saisivat lainsoveltajina toimintaansa riittävät valtuudet. [KM 1981/66]

Suomalainen tietosuojalainsäädäntö kuuluu myös välineneutraaliksi nimitettävään lainsäädäntöön. Henkilötietojen käsittelyn tekniikat kehittyvät nopeasti, joten lakisäännökset on kirjoitettu siten, ettei sanamuotoja ole sidottu tietynlaiseen tekniikkaan. [HE 96/1998] Henkilötietojen käsittely ja tietoturvallisuuden arviointi jäävät näin ollen lain peruskäsitteiden ja yleissäännösten varaan, käsittely-ympäristöstä riippumattomiksi. Esimerkiksi Internetin varalle ei ole tehty erityissäännöksiä. [Saarenpää, 2004]

Tietosuojalainsäädännön väljyyttä ja sen jättämää tulkinnanvaraa on vuoroin kiitelty ja moitittu. Sekä henkilörekisteri- että henkilötietolain yleispiirteisyyttä on ajateltu täydennettävän erityislainsäädännössä toteutettavilla erikoissäännöksillä. Muun muassa Partanen [1995] on arvostellut tällaista ratkaisua. Ilman asiallisia perusteluja säännösten syrjäyttäminen erityissäännöksillä voi perustua puhtaaseen vallankäyttöön.

Lisäksi Partasen [1995] mielestä yksityisyyttä ja sen mahdollisia loukkauksia tulisi selventää. Lainsäädännössä yksityisyyden suoja on määrittelemisen sijasta pitkälti toiminnallistettu. Tämä johtaa kaavamaisuuteen laintulkinnassa, mikä puolestaan on omiaan lisäämään ymmärtämättömyyttä tietosuoja-asioita kohtaan. Suoranaiseksi epäselvyyden lähteeksi Partanen [1996] mainitsee lain soveltamisalan laajuuden. Henkilötietodirektiivin myötä henkilötiedon käsite on laajentunut eikä tietosuojaongelmia kytketä enää pelkkään rekisterinpitoon vaan yleisesti henkilötietojen käsittelyyn. Tietosuoja-asioiksi mielletyt kysymyksetkin laajentuvat näin entisestään, ellei lainsäädännössä tarkemmin yksilöidä yksityisyyden suojaa loukkaavaa henkilötietojen käsittelyä. Mahkonen [1997] puolestaan on tutkinut yksityisyyden suojan sääntelyä lainsäädännössä kauttaaltaan, pelkkää tietosuojalainsäädäntöä laajemmin. Hän on kiinnittänyt huomiota yksityisyyden suojan normittamiseen toisistaan poikkeavin tavoin. Mahkosta lainaten: "Yksityisyyttä säännellään laajasti, epäjohdonmukaisesti ja utuisasti", eikä lainsäätäjä ole ottanut kantaa siihen, miten vastakkaisten oikeusohjeitten välille tulisi hakea tasapainotilaa.

Tietosuojariskejä arvioitaessa yhtenä riskinä voidaan Partasen [1996] mukaan pitää sitä, ettei riskeistä tiedetä tarpeeksi eikä niitä tällöin voida ennaltaehkäistä. Juuri siksi

Partasen mielestä tietosuojakysymyksissä tulisi aina selventää, miten yksityisyyden suoja on kulloinkin uhattuna. Vaikka lainvalmistelutöissä ei ole mahdollista perehtyä kovin syvällisesti yksittäisiin kysymyksiin, tulisi edes yksityisyyden suojan ydinalue määritellä — lainvalmistelussahan kuitenkin muotoillaan ja kehitetään tietosuoja-ajattelua.

Saarenpää [2004] arvioi, että välineneutraali henkilötietolaki periaatteessa soveltuu hyvin henkilötietojen käsittelyyn tietoverkossa. Vanhassa henkilörekisterilaissa oli kuitenkin erityinen massaluovutuksia sääntelevä pykälä. Uudesta henkilötietolaista tämä käsite ja massaluovutuksen erityisrajoitukset jätettiin pois. Oikeudellisesti, henkilötietolain tulkinnan kannalta, on toki edelleen selvää, että hakukelpoisten henkilötietojen asettaminen Internetiin merkitsee näiden tietojen luovuttamista. Saarenpää arvostelee silti massaluovutussäännöksen poisjättämistä, sillä käytännössä maallikko ei miellä tietojen verkkoon laittamista luovutukseksi ja sen vuoksi laki olisi saanut olla informatiivisempi. Osaksi asiaan on vaikuttanut uuden julkisuuslain säätäminen, sillä julkisuuslaissakaan ei ole erityissäännöksiä henkilötietojen käsittelystä avoimessa tietoverkossa. Näin on päädytty tilanteeseen, jossa henkilötietoja luovutetaan verkkoon julkisuuden ja avoimuuden nimissä miettimättä yksityisyyden merkitystä.

Välineneutraali tietosuojalainsäädäntö vaikuttaa perustellulta ratkaisulta, sillä teknologiaan kantaa ottavaa lainsäädäntöä uhkaa pikainen vanhentuminen. Tietosuojalainsäädännössä on esitetty selkeät perusperiaatteet, jotka soveltuvat henkilötietojen käsittelyyn erilaisissa ympäristöissä. Lain sisällön sijasta ongelmana on, ettei laissa esitetty rekisterinpitäjän itseohjautuvuus toteudu. Lakia ei noudateta, toisinaan tietämättömyydestä, mutta yhä useammin silkasta välinpitämättömyydestä. Koska verkkopalveluiden suunnittelijat ja ylläpitäjät eivät vaikuta halukkailta noudattamaan lakia vapaaehtoisesti, tulisi lain valvontaa kehittää ja mahdollisuuksien mukaan automatisoida — vastattakoon siis tekniikan kehitykseen tekniikalla.

4. Henkilötietolaki ja tietosuojaperiaatteet www-sivustoilla

Tietosuojavaltuutettu Jorma Kuopus on toimintakautenaan ottanut kantaa verkkosivustoilla vallinneeseen tapaan kerätä palveluiden käyttäjien henkilötietoja. Kuopuksen käsitys on ollut, että on-line-palveluissa tulee välttää henkilötietojen keräämistä ja käsittelyä mahdollisuuksien mukaan. Mikäli tietoja on rekisteröitävä, on hyvän rekisteritavan [nykyisin siis hyvän tietojenkäsittelytavan] mukaista tyytyä vain minimitietoihin. [Kuopus, 1997a; Tietojen rekisteröinti..., 1997]

4.1. Oikeus yksityisyyden suojaan

Wallin ja Nurmi [1991] ovat määritelleet, että tietosuojaan kuuluu muun muassa informaation pitäminen poissa asiaankuulumattomien käytöstä. Verkkopalveluissa tämä tarkoittaa sellaisten järjestelmien toteuttamista, jotka eivät mahdollista sivullisten pääsyä käyttäjän henkilötietoihin.

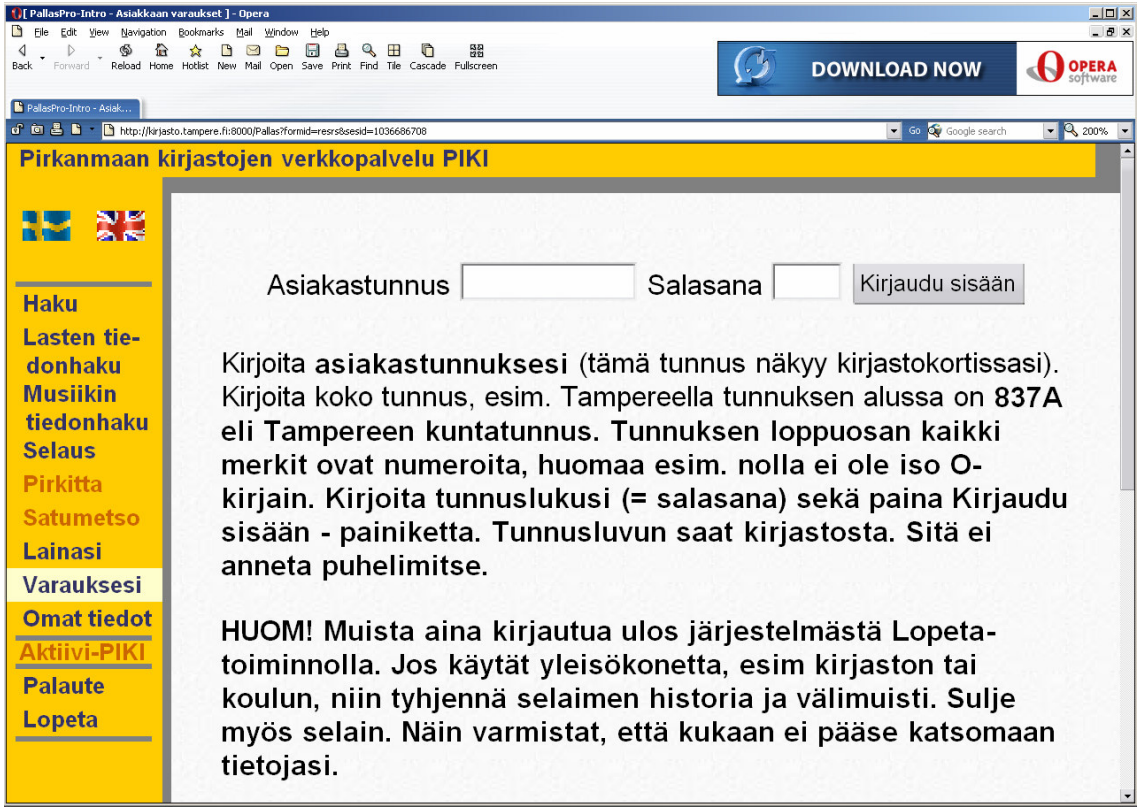
Pirkanmaan kirjastoilla on yhteinen Piki-verkkopalvelu[3], jossa kirjaston asiakas voi asiakastunnuksen ja salasanan yhdistelmällä käsitellä omia kirjaston käyttöön liittyviä tietojaan. Myös kirjastojen yleisissä tiloissa on runsaasti PC-työasemia, joilta asiakkaat käyttävät palvelua Internet-yhteyden kautta. Pirkanmaan maakuntakirjastolla on kymmeniä tuhansia asiakkaita, ja verkkokirjaston mahdollistama itsepalvelu on suosittua, joten kirjastojen asiakaskäytössä olevilla työasemillakin lienee satoja viikoittaisia käyttäjiä.

Navigointi palvelussa on toteutettu sivuston vasemmassa marginaalissa sijaitsevalla linkkilistalla (Kuva 1). Omat tiedot -linkki johtaa asiakkaan henkilötietoihin, joihin kuuluvat muun muassa nimi, osoite, maksamattomat maksut ja huomautukset sekä salasanan vaihto. Lainasi- ja Varauksesi-linkkien takaa löytyvät puolestaan asiakkaan lainaus- ja varaustiedot. Kirjauduttuaan palveluun käyttäjä voi esimerkiksi uusia omia lainojaan sekä tehdä ja poistaa varauksia kirjaston aineistoon. Mikäli käyttäjä valitsee vasemman marginaalin Lopeta-linkin, tulostaa palvelu ilmoituksen: "Käyttämäsi istunto on lopetettu."

Lopeta-linkin valitseminen ei todellisuudessa hävitä istunnon tietoja kuten käyttäjä saattaisi täysin oikeutetusti olettaa. Sen sijaan selaimen Takaisin-painikkeella (*Back*) saadaan näkyviin sivu sivulta istunnon koko historia, aineistohaut mukaan lukien. Piki-verkkopalvelu on ollut käytössä vuosia, ja ongelmakin lienee tullut jo ilmi. Nykyisin "Käyttämäsi istunto on lopetettu" -palautteen lisäksi sivulle tulostetaan myös ohjeistus: "Jos haluat varmistaa ettei kukaan pääse edes vahingossa katselemaan laina- tai varauslistaasi kannattaa selain sulkea." Ohje jatkuu: "Varmin tapa hävittää kaikki istunnon tiedot Tampereen kaupunginkirjaston laitteilla on käyttää Käynnistä-palkin alta Reboot-toimintoa. Jos käytät yleisessä tilassa olevaa työasemaa, esim. kirjastossa tai koulussa, tietoihisi ei pääse enää käsiksi ilman tunnuksiasi." Tekstillä tarkoitettaneen sitä, etteivät

[3] http://kirjasto.tampere.fi:8000/

tiedot ole muiden saatavilla, mikäli työasemaan on kirjauduttu henkilökohtaisella käyttäjätunnus ja salasanaparilla — edellyttäen tietysti, että käyttäjä on kirjautunut myös ulos. Ohjeistus on kuitenkin mahdollista tulkita virheellisesti. Hämmennystä lisännee palvelun sisäänkirjautumisen yhteydessä annettava ohje, jossa todetaan: "Jos käytät yleisökonetta, esim kirjaston tai koulun, niin tyhjennä selaimen historia ja välimuisti. - - Näin varmistat, että kukaan ei pääse katsomaan tietojasi." (Kuva 1)



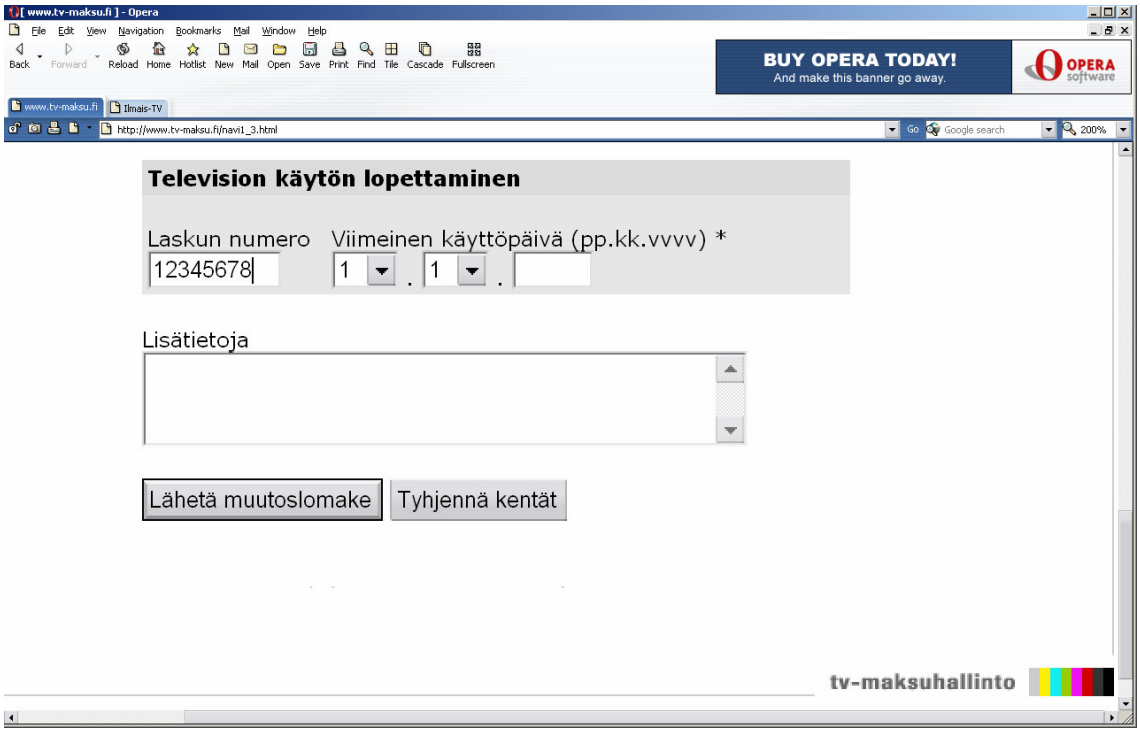
Kuva 1. Piki-verkkokirjaston sisäänkirjautumissivu sisältää ohjeistusta palvelun käytöstä. Palvelussa navigoidaan vasemmassa marginaalissa sijaitsevilla linkeillä.

Käytännössä on varsin tavallista, että Piki-verkkopalvelua kirjastossa käyttänyt asiakas yksinkertaisesti jättää selaimen auki painettuaan Lopeta-linkkiä. Näin palvelun käyttäjien yksityiselämään liittyviä tietoja on kirjastoissa päivittäin saatavilla. Henkilötietolain periaatteiden lisäksi palvelu rikkonee myös sähköisen viestinnän tietosuojalain 4. §:ssä säädettyä luottamuksellisen viestin suojaa. Sivustoon liitetystä linkistä päätellen palvelun on toteuttanut "Pohjoismaiden suurin tietotekniikan palveluyritys" TietoEnator.

4.2. Tietojen laadun varmistaminen

Rekisterinpitäjälle on asetettu lakisääteinen vaatimus huolehtia rekisteröitävien tietojen virheettömyydestä. Verkkopalveluissa rekisterinpitäjän tulisi ensisijaisesti varmistaa, että palvelun käyttäjän on mahdollista antaa virheettömiä ja oikeita tietoja. Tietojen syöt-

töön käytettävien lomakkeiden onnistuneisuutta ei voi arvioida pelkästään lomakkeen ulkonäön perusteella, sillä verkkolomakkeiden käyttökelpoisuus varmistuu vasta testauksen jälkeen. Puutteellisen teknisen toteutuksen seurauksena käyttäjälle voi olla jopa mahdotonta syöttää tietoja oikein. Lomakekentälle on saatettu esimerkiksi määritellä maksimipituus, jonka ylittävää syötettä kenttä ei ota vastaan, vaikka todellinen tarve vaatisi toisin. Esimerkiksi Viestintäviraston verkkopalvelussa on lomakekenttä, joka ei ota vastaan riittävän pitkää syötettä. Postitse tulleessa televisiomaksussa laskun numero on 11 merkin pituinen — lomakekenttään on kuitenkin mahdollista syöttää vain 8 merkkiä. (Kuva 2).



Kuva 2. Esimerkki liian lyhyestä syötekentästä (http://www.tv-maksu.fi/navi1_3.html).

Toisinaan kentät on ohjelmoitu siten, että käyttäjä ei tiedä syötteen pituusrajoitusta. Kenttään näyttää mahtuvan merkkejä loputtomasti, vaikka todellisuudessa lomakkeen lähetyksessä syöte katkaistaan jostakin kohdasta. Palvelun käyttäjä ei puolestaan voi olla tästä tietoinen, ellei hänelle anneta palautetta liian pitkästä syötteestä. Huonosti suunniteltu tai vanhentunut verkkolomake voi aiheuttaa tiedon laatuun liittyviä ongelmia, joten lomakkeiden toteutukseen ja ylläpitoon kannattaa kiinnittää erityistä huomiota.

4.3. Informointivelvoitteen täyttäminen

Henkilötietolain 10. §:n mukaan jokaisesta rekisteristä on laadittava rekisteriseloste. Rekisterinpitäjän tulee pitää rekisteriselostetta toimipaikassaan jokaisen saatavilla — verkkopalvelussa tämä merkitsee sitä, että selosteen on löydyttävä verkosta. Yleinen re-

kisteriselostemalli on saatavissa tietosuojavaltuutetun toimiston verkkosivuilta[4]. Rekisteriselosteen täyttämisen lisäksi henkilötietoja keräävän tulee lain 24. §:n mukaisesti informoida rekisteröityjä heidän henkilötietojensa käsittelystä.

Informoinnin on oltava käsillä, kun asiakas suunnittelee verkkokaupassa tilauksen tekemistä tai palvelun käyttäjäksi rekisteröitymistä (Kuva 3). Samassa yhteydessä on kerrottava mahdollisuudesta kieltäytyä suoramarkkinoinnista sekä siitä, miten tämä kielto on toteutettavissa. Informointi voidaan toteuttaa linkillä, joka johtaa rekisteriselosteeseen sekä muihin informointitietoihin.

Kuva 3. Aamulehden verkkopalvelun käyttäjäksi rekisteröitymisen yhteyteen on koottu linkit, jotka täyttävät rekisterinpitäjälle säädetyn informointivelvoitteen.

[4] http://www.tietosuoja.fi/2584.htm

Informointivelvoite täyttyy, kun rekisteröitävä saa seuraavat tiedot:
— kuka rekisterinpitäjä on (nimi ja yhteystiedot)
— mikä on rekisterin käyttötarkoitus
— henkilötietojen suojaamisen periaatteet
— mihin rekisteröityjen henkilöiden tietoja säännönmukaisesti luovutetaan
— tiedot siitä, miten rekisteröityjen oikeudet on toteutettu.
Markkinointikiellon tekemisen lisäksi rekisteröidyllä on oikeus tarkastaa itseään koskevat tiedot sekä vaatia rekisterissä olevan virheellisen tiedon oikaisua. [Näkökohtia henkilötietojen..., 2002]

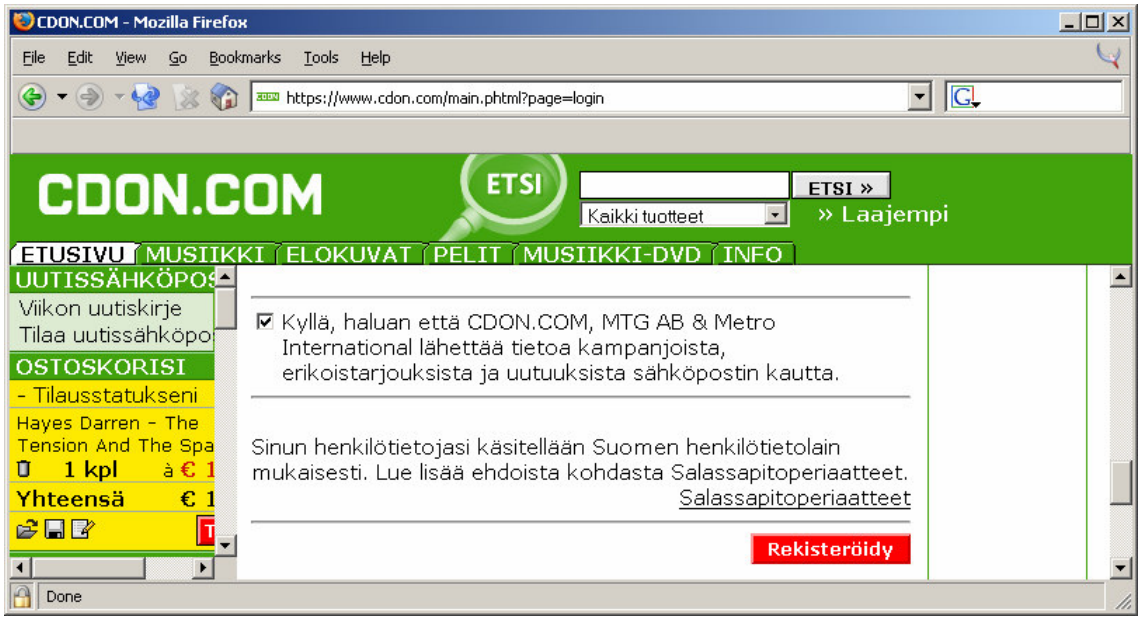
4.4. Kielto-oikeuden käyttäminen

Tietosuojavaltuutettu Jorma Kuopus on esittänyt, että verkkopalvelun käyttäjäksi rekisteröityvälle on varattava tilaisuus kieltää henkilötietojensa käyttö suoramarkkinointiin ja markkinatutkimukseen hiiren klikkauksella [Kuopus, 1997a]. Vastaavasti tilaus- ja arvontakuponkeja koskevassa kannanotossaan Kuopus on kiinnittänyt huomiota kielto-oikeuden käyttämisen tapaan, jonka tulisi olla mahdollisimman tarkoituksenmukainen ja yksinkertainen. Esimerkiksi tilaus- ja arvontakuponkien yhteyteen tulisi varata mahdollisuus käyttää kielto-oikeutta. Kuopuksen mielestä on kohtuutonta edellyttää, että rekisteröity itse oma-aloitteisesti ottaisi yhteyttä rekisterinpitäjään joko kirjallisesti tai puhelimitse suoramarkkinointikielto-oikeutta käyttääkseen. Kohtuutonta vaivannäköä korostaa se, että tilaus- ja arvontakuponkeihin on helposti lisättävissä erillinen kohta, esimerkiksi rastitettava ruutu, jolla kielto-oikeuden käyttämisen voi ilmaista. [Hyvään rekisteritapaan..., 1997]

Internet-sivustoilla Kuopuksen esittämät periaatteet voisivat toteutua esimerkiksi siten, että rekisteröitymisen tai tilauksen tekemisen yhteyteen liitettäisiin kaksi kielto-oikeuden käyttämistä ilmaisevaa valintaruutua (*checkbox*). Toiseen ruutuun voidaan liittää teksti: "Kiellän henkilötietojeni käytön ja luovuttamisen suoramarkkinointiin." Toisen yhteydessä voi puolestaan lukea: "Kiellän henkilötietojeni käytön ja luovuttamisen markkina- ja mielipidetutkimuksiin." Tekstien perään kannattaa liittää viite henkilötietolain 30. §:ään. Esimerkiksi Alma Media Oy on hoitanut Internet-palveluidensa käyttäjäksi rekisteröityvien informoinnin henkilötietolain vaatimusten mukaisesti. Yritys ei kuitenkaan varaa asiakkailleen mahdollisuutta kieltää suoramarkkinointia rekisteröitymisen yhteydessä, kuten verkkosivustolla olisi luontevinta. Sen sijaan kielto-oikeuttaan käyttävän on tehtävä asiasta kirjallinen ilmoitus rekisterinpitäjän ilmoittamaan osoitteeseen [http://guard.almamedia.fi/aa/perustiedot.html?SERVICE_ID=20, linkki "käyttösopimuksen"].

Verkkosivustoilla on myös tyypillistä esittää kielto-oikeus ikään kuin käänteisessä muodossa. Henkilötietojen antamisen yhteydessä ei kerrota oikeudesta kieltäytyä suoramarkkinoinnista — sen sijaan asia esitetään tekstimuodossa "Haluan, että minulle lähetetään..." tai "Kyllä kiitos, lähettäkää minulle..." Vaikutelmaa tehostetaan vielä käyt-

täjän puolesta valituksi merkityllä valintaruudulla (Kuva 4). Tietosuojalautakunnan antaman päätöksen mukaan rekisteröidylle on annettava oikea ja selkeä kuva tämän oikeuksista [Hyvään rekisteritapaan..., 1997]. Käyttäjän puolesta tehdyt valinnat suoramarkkinoinnin vastaanottamiseksi eivät toteuta hyvää tietojenkäsittelytapaa.



Kuva 4. Esimerkki käänteisessä muodossa ilmaistusta kielto-oikeudesta.

4.5. Tietosuojavaltuutetun toimiston tekemä selvitys

Tietosuojavaltuutetun toimisto teki vuonna 2002 selvityksen verkkopalveluiden käyttäjien henkilötietojen keräämisestä ja tietojen käytön informoinnista. Tutkimuksen tuloksista on kerrottu Tietosuoja-lehdessä. Selvityksessä oli mukana 478 suomalaista sivustoa, jotka jaettiin kuuteen kategoriaan: valtion-, kunnallis- ja muuhun julkiseen hallintoon, järjestöihin, yrityksiin sekä verkkolehtiin. Henkilötietoja keräämiä toimintoja oli ryhmitelty 13 luokkaan: palaute/kysymyslomake, vieraskirja ja aloitteet, asiakaskysely, tilauslomake, ilmoittautuminen, asiointipalvelu, työpaikkailmoitus/-hakemus, nettipostikortti, verkkokauppa, ilmoitustaulu, postituslista, keskustelupalsta sekä palveluun rekisteröityminen. [Kara, 2002]

Henkilötietoja kerättiin eniten palaute- ja kysymyslomakkeilla, joita oli sivustoista lähes 80 prosentilla. Kara [2002] toteaa, että vain harvat palautelomakkeet toimivat anonyymisti — kommentti tosin jättää epäselväksi, olisiko otoksessa mukana olleilla lomakkeilla ollut mahdollista lähettää pelkkä palauteteksti ilman henkilötietoja. Käytännössä asialla ei liene suurta merkitystä, sillä jo pelkästään henkilötiedoille varatut lomakekentät saattavat ohjata käyttäjän olettamaan, että kaikki tiedot on täytettävä.

Verkkolehdiksi luokitellut palvelut saivat tutkimuksen parhaan tuloksen, sillä lehdistä lähes 77 prosenttia informoi käyttäjiään heidän henkilötietojensa käsittelyn periaatteista. Seuraavaksi parhaita informoijia olivat yritykset 49 prosentin tuloksella. Jär-

jestöistä lähes 23 prosenttia hoiti velvoitteensa. Huonoimmin käyttäjiään informoivat julkisen hallinnon palveluntarjoajat, joista surkeimmin selvisi muuksi julkiseksi hallinnoksi luokiteltu taho 5,9 prosentin tuloksella. Tähän kategoriaan kuuluivat esimerkiksi Kela ja Suomen Pankki. Muut julkishallinnon sivustot eivät pärjänneet paljoakaan paremmin, sillä kunnallishallinnon tulos oli 14,6 prosenttia ja valtion hallinnon 10 prosenttia. [Kara, 2002]

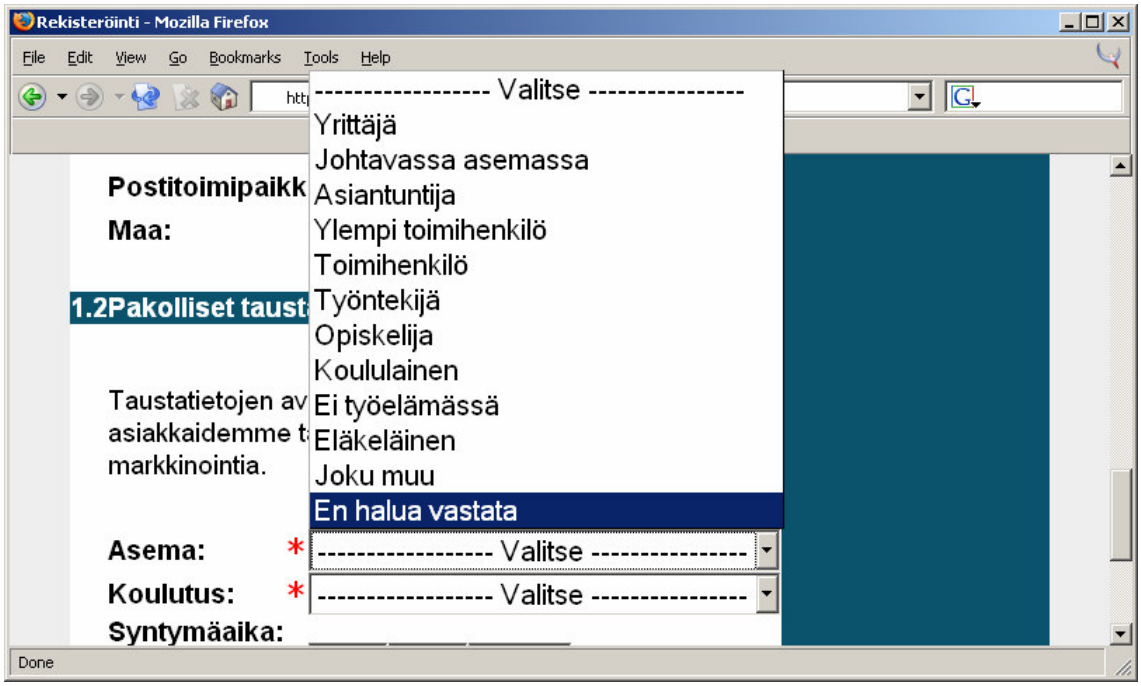
Tietosuoja-lehden julkaisemissa tutkimustuloksissa ei kerrota, tehtiinkö informointivelvoitteen täyttämisestä myös laadullista analyysiä. Epäselväksi jää sekin, onko informoinniksi laskettu myös puutteellisesti hoidettu velvoite. Rivien välistä luettaessa näin näyttäisi olevan, sillä esimerkiksi järjestöjen kohdalla mainitaan: "Luvan kysyminen suoramarkkinointiin tai ilmoitus mahdollisuudesta kieltää suoramarkkinointi on näiden verkkopalvelusivujen yleisin henkilötietojen käyttöä kuvaava tieto." [Kara, 2002] Kielto-oikeudesta kertominenhan kattaa vain informointivelvoitteen yhden osan. Lainauksesta ei selviä sekään, onko kielto-oikeuden käyttömahdollisuus konkreettisesti toteutettu esimerkiksi lomakkeella olevalla valintaruudulla, jonka rastittamalla käyttäjä voi osoittaa käyttävänsä oikeuttaan. Tietosuoja-lehden artikkelista ei myöskään ilmene, onko selvityksestä tehty muita päätelmiä kuin seuraava: henkilötietojen keruu on yleistä, mutta niiden käytöstä informointi vähäistä.

Julkisen hallinnon erittäin huonosti hoitamaan informointivelvoitteen täyttämiseen on vaikea keksiä selitystä. Käyttävätkö julkiset rekisterinpitäjät röyhkeästi hyväkseen sitä, että ne joutuvat toimistaan hyvin harvoin rikosoikeudelliseen vastuuseen? Julkisten tahojen välinpitämättömyyttä korostaa se, että tietosuojavaltuutetun toimisto oli vuotta ennen selvityksen tekoa lähettänyt valtion ja kunnan eri organisaatioille, korkeakoulujen johdolle ja suurimmille kansalaisjärjestöille kirjeen, jossa painotettiin rekisterinpitäjän informointivelvoitetta [Kara, 2002]. Pohdittavaksi jää, onko kirjeellä ollut näihin rekisterinpitäjiin ollenkaan vaikutusta, vai olisiko tulos ollut ilman tiedotetta vieläkin huonompi. Suurimmilla julkisilla laitoksilla on yleensä sekä lakimiespalvelut että organisaation verkkopalveluista vastaavat viestintä- ja tietohallinto-osastot, joten informointivelvoitteen laiminlyöntiä tuskin voi selittää tietämättömyydellä tai resurssipulalla.

Verkkolehdiksi luokitellut palvelut ovat selvityksen mukaan hoitaneet informointivelvoitteen hämmästyttävän hyvin muihin verkkosivustoihin verrattuna. Tulosta voitaneen selittää sillä, että tietosuojavaltuutettu Jorma Kuopus otti tutkittavakseen omasta aloitteestaan Aamulehden verkkosivuston lukijoiden rekisteröimiskäytännön jo vuonna 1996. Lisäksi valtuutettu on arvostellut Aamulehden, Iltalehden ja Kauppalehden tapaa kerätä lukijoiksi rekisteröityvistä varsin yksityiskohtaisia tietoja — esimerkiksi Aamulehti halusi tietää, onko lukija työtön. Kuopuksen [1997a] mukaan verkkoympäristössä tulisi olla anonyymin lukemisen oikeus.

Nykyisin Aamulehden lukijaksi rekisteröityvä voi jättää vastaamatta muun muassa asemaa ja koulutusta koskeviin tietoihin (Kuva 5). Taustatiedot tosin ilmoitetaan pakol-

lisiksi vaikka vaihtoehdoista lopulta löytyy myös "En halua vastata". Epäselväksi jääkin, miksi tiedot on merkitty pakollisiksi tämänkin vaihtoehdon ollessa mahdollinen.



Kuva 5. Aamulehden lukijaksi rekisteröityvältä kysytään muun muassa asemaan ja koulutukseen liittyviä tietoja "pakollisina taustatietoina".

Verkkolehdet ovat siis joutuneet tietosuojavaltuutetun erityisen huomion kohteeksi ja korjanneet sittemmin toimintatapojaan. Suurimmilla lehdillä lienee omat lakimiespalvelut, joten lukijaksi rekisteröitymisen ehdot ovat usein varsin huolellisesti laadittuja. Koska useimmilla verkkolehdillä on sama palveluformaatti, on pienempien lehtien helppo seurata suurempien antamaa esimerkkiä ja soveltaa samoja käytänteitä.

4.6. Henkilötietojen julkaiseminen verkossa

Henkilötietojen julkaiseminen Internetissä merkitsee henkilötietojen sähköistä luovuttamista. Tietosuojaviranomaisten kannanottojen mukaan henkilötietoja ei saa tunnistettavassa muodossa laittaa Internetin kotisivuille ilman asianomaisen henkilön antamaa suostumusta [Ammattiyhdistyksen jäsenten..., 2003; Opiskelijoiden kurssiarvostelujen..., 2001]. Suostumuksen on mieluiten oltava kirjallinen [Puukka, 2001]. Suostumuksen tarvetta perustellaan muun muassa sillä, ettei tietoja luovuttava rekisterinpitäjä enää hallitse tietojen käyttöä. Luovutuksensaajia ei voida määritellä tarkasti, sillä heitä ovat kaikki Internetiä käyttävät. Selvitettävissä ei myöskään ole, mitä luovutuksensaaja aikoo saamillaan henkilötiedoilla tehdä. [Oppilaiden henkilötietojen..., 2002]

Henkilötietojen käsittelyyn liittyy myös käyttötarkoitussidonnaisuuden periaate, joten suostumus ei välttämättä yksin riitä henkilötietojen julkaisuun verkossa. Tietosuojaviranomaiset kyseenalaistavat esimerkiksi oppilasrekisteriin sisältyvien henkilötietojen

viemisen koulun kotisivuille, sillä oppilaitoksissa oppilaiden henkilötietojen käsittelyn peruste on opetuksen järjestäminen. [Oppilaiden henkilötietojen..., 2002] Vastaavasti yhdistystoiminnassa henkilötietojen laittamista Internetiin ei voida perustella pelkästään yhdistyksen jäsenten välisen yhteydenpidon helpottamisella [Puukka, 2001].

4.7. Käytännesäännöt

Henkilötietolain 42. §:ssä säädetään toimialakohtaisista käytännesäännöistä. Käytännesääntöjen tarkoituksena on, että rekisterinpitäjät laatisivat itse säännöt, jotka edistävät hyvän tietojenkäsittelytavan noudattamista kyseisellä toimialalla. Tietosuojavaltuutettu voi antaa sääntöjen laatimiseen ohjeita sekä varmistaa niiden lainmukaisuuden. Sääntöjen luominen on toistaiseksi vapaaehtoista. [HE 96/1998] Myös sääntöjen oikeudellinen merkitys on vielä avoin puuttuvan oikeuskäytännön vuoksi [Niku-Paavo, 2003]. Tiedossa ei siis ole, mitä sääntöjen rikkomisesta tai noudattamatta jättämisestä oikeudellisessa mielessä seuraa, ja kuinka sitovina sääntöjä voidaan pitää.

Käytännesäännöillä yleisluonteisen ja paikoin vaikeaselkoiseksi koetun henkilötietolain sisältö tulee helpommin omaksuttavaksi ja kansantajuisemmaksi. Samalla voidaan ottaa huomioon tietyn alan erityiset piirteet henkilötietolakia sovellettaessa. Säännöt luovat yhteisesti hyväksyttyjä tulkintoja lain sisällöstä. Lain sisällön muuttuessa konkreettisemmaksi, paranee samalla kansalaisten oikeuskäsityskin. Parhaimmillaan säännöt myös hidastavat tai jopa estävät lakisäädösten määrän kasvua. [Niku-Paavo, 2003] Tietosuojavaltuutetun toimisto on julkaissut ohjeistuksen käytännesääntöjen laatimisesta[5].

Saarenpää [2004] pitää käytännesääntöjä yhtenä henkilötietodirektiivin hienoimmista oivalluksista. Hän kuitenkin huomauttaa, että kaikki tähän mennessä luodut käytännesäännöt ovat olleet jälkikäteisiä. Mikäli käytännesäännöt luodaan jälkikäteen ja suunnittelun pohjana on ollut lainvastainen käytäntö, seuraa siitä yksityisyyden suojan vaarantumista. Erityisesti tietojärjestelmiin liittyvien käytännesääntöjen kohdalla sääntöjen valmistelu tulisi aloittaa yhdessä tietojärjestelmän suunnittelun kanssa, jotta jatkossa vältyttäisiin kalliiksi tulevilta systeemiongelmien korjauksilta. Lisäksi Saarenpään mielestä on tärkeää, että tietosuojavaltuutettu osallistuisi sääntöjen valmisteluun mahdollisimman varhaisessa vaiheessa — muutoin on vaarana, että rekisterinpitäjä voi yrittää jopa tarkoituksellisesti vakiinnuttaa yksityisyyden vastaisia käytänteitä.

Saarenpään huoli ei vaikuta aiheettomalta. Esimerkiksi Kuluttajavirasto on antanut 28.1.2004 lausunnon Väestörekisterikeskukselle yksityisen sektorin tietopalvelun käytännesäännöistä. Asia koskee sääntöjen kohtaa 8.1.2, jossa ohjeistetaan alle 18-vuotiaiden poimintaa väestötietojärjestelmästä suoramainontaa varten. Lausunnossa todetaan sääntöjen olevan ristiriidassa kuluttaja-asiamiehen näkemyksen kanssa. Lisäksi säännöissä jätetään kuluttaja-asiamies ja kuluttajansuojasäännökset mainitsematta, vaikka kuluttaja-asiamies valvovana viranomaisena antaa ohjeita ja ratkaisuja nimenomaan

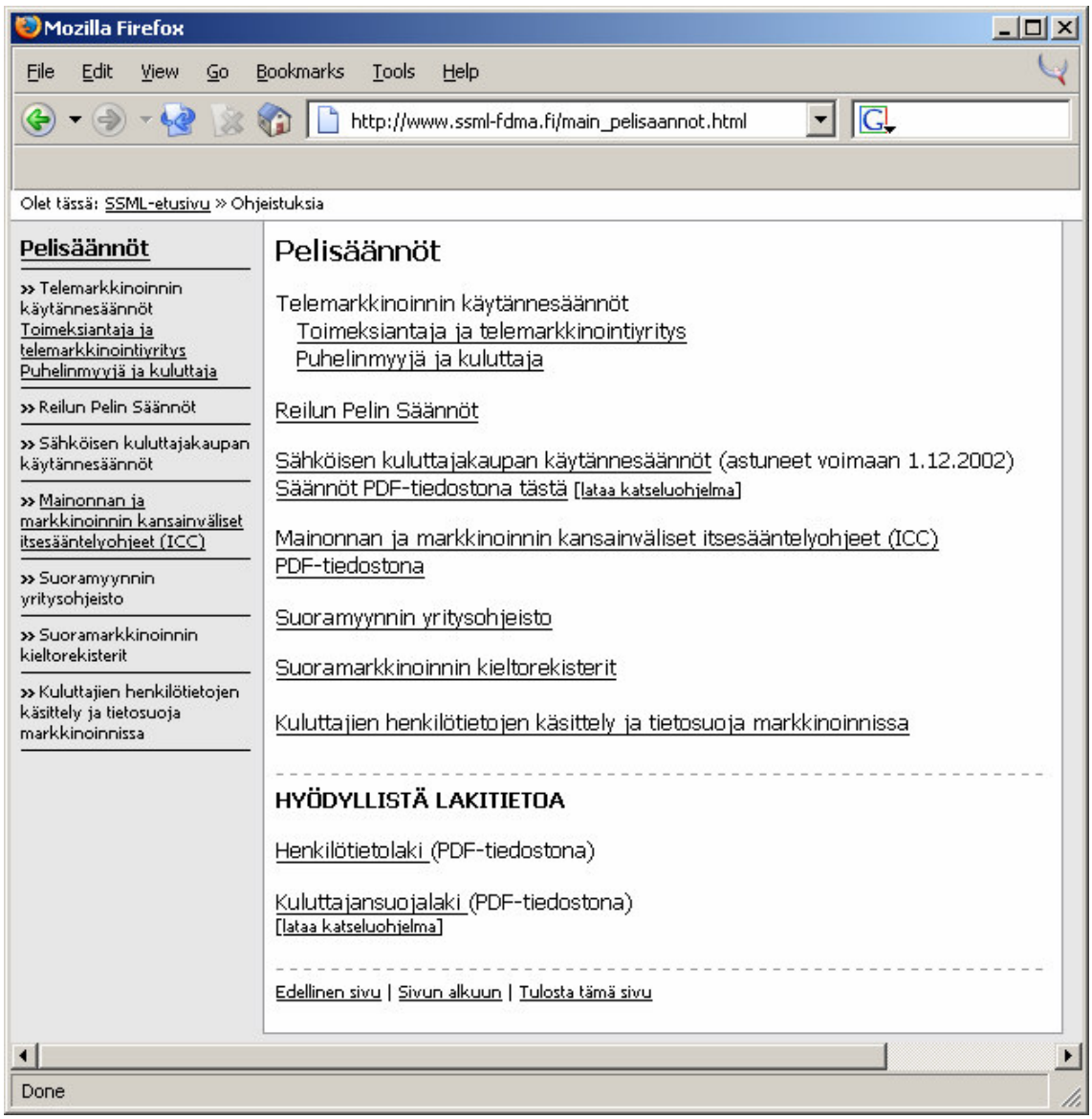
[5] http://www.tietosuoja.fi/9291.htm

markkinointia koskevissa asioissa. Lausunnossa huomautetaan, että kuluttajaviranomaiset on mainittava kyseisissä käytännesäännöissä. [Lausunto Väestörekisterikeskukselle..., 2004]

Toisessa esimerkissä arvostellaan Suomen Suoramarkkinointiliiton, Kaupan Keskusliiton, Keskuskauppakamarin sekä tietoliikenteen ja tietotekniikan keskusliiton FiComin laatimia sähköisen kuluttajakaupan käytännesääntöjä. Electronic Frontier Finland (EFFI) ry valvoo kansalaisten oikeuksia Internetissä. Yhdistys on huomannut sähköisen kuluttajakaupan säännöistä kohdan, jossa väitetään, että yritys voi pyytää kuluttajalta suostumuksen suoramarkkinointiin automaattista televiestintää käyttämällä — siis esimerkiksi sähköpostitse tai tekstiviestillä. Samassa yhteydessä voisi sääntöjen mukaan kuvata, millaisia tuotteita yritys markkinoisi. [Uudet sähköisen..., 2002] Markkinaoikeus on 19.6.2003 antanut päätöksen, jonka mukaan myös sellaiset sähköiset viestit, joissa pyydetään lupaa mainosten lähettämiseen, ovat itsessään suoramarkkinointia [MAO: 119/03]. Sähköisen kuluttajakaupan käytännesäännöt antavat siis laitonta ohjeistusta.

Hakusanalla "käytännesäännöt" Google-hakupalvelu antaa tulokseksi kymmenisen linkkiä henkilötietolain tarkoittamiin käytännesääntöihin. Hakutulosten perusteella sääntöjen laatimisessa ovat parhaiten kunnostautuneet suoramarkkinointiin liittyvät tahot. IT-alan sääntöjä ei sen sijaan tulosten joukosta löydy sähköistä kauppaa lukuun ottamatta. On tietysti mahdollista, ettei sääntöjä ole julkaistu verkossa, vaikka juuri IT-alan ohjeistusten kuvittelisi Internetistä löytyvän. Tietosuojavaltuutetun toimiston päivämättömällä sivulla [http://www.tietosuoja.fi/1696.htm] todetaan: "Sivua tullaan täydentämään luettelolla tähän mennessä laadituista käytännesäännöistä." Luetteloa ei kuitenkaan sivulla ole, vaikka sääntöjä on jo laadittu ja tietosuojavaltuutetun toimistossakin tarkastettu.

Suomen Suoramarkkinointiliitto ry (SSML) on kunnostautunut esimerkillisesti erilaisten toimintasääntöjen laatimisessa. SSML:n verkkosivuille on koottu runsaasti sekä kuluttajia että suoramarkkinoijia hyödyttävää ohjeistusta (Kuva 6). Verkosta löytyy myös vakuutusalan käytännesääntöjä. Sekä suoramarkkinointi- että vakuutusala ovat kumpikin toimialoja, joilla kuluttajien tunteet perinteisesti kuumenevat. Esimerkiksi vuonna 1996 tietosuojavaltuutetun tutkimista asioista 6—7 % koski suoramainontaa [Kuopus, 1997a]. On siis ymmärrettävää, että huonon maineen uhatessa kyseisillä aloilla on katsottu parhaaksi luoda reilun pelin sääntöjä. Samalla tämä osoittaa sen, että yleisöpaine vaikuttaa yritysten käytänteisiin.



Kuva 6. Suomen Suoramarkkinointiliitto ry:n kokoamia ohjeita (http://www.ssml-fdma.fi/main_pelisaannot.html).

5. Tietoverkkojen yleistymisestä seuranneita ilmiöitä

Tietojenkäsittelyn tavanomaistuttua on jouduttu sopeutumaan uudenlaisiin tapoihin toimia. Saarenpään [2004] mielestä lainsäätäjänkin tulisi ymmärtää, ettei tietojenkäsittely ole enää pelkkä apuväline, vaan asia johon olemme sidoksissa. Yhä useampi toiminto on perusteltua nähdä oikeudellisesti merkityksellisenä informaatioprosessina, joka alkaa esimerkiksi yrityksen tai julkisen palvelun kotisivun avaamisella. Henkilötietolaissa, tietojärjestelmäsuunnittelusta puhumattakaan, ei ole riittävästi varauduttu siihen, että perusoikeudet tulisi huomioida jo prosessin alusta alkaen.

5.1. Rekisterinpidon muuttunut luonne

1980-luvulta peräisin olevissa tietosuojasäännöksissä henkilörekisterinpitäjää käsitellään ennalta määrättynä tahona, joka on myös rekisteröitävien tavoitettavissa. Myös henkilötietojen käsittelyä pidetään tarkoin määriteltävänä ja yksityiskohtaisesti vaiheistettavana toimintana. Tietojen käsittelyyn käytettävät laitteet ja niiden sijainti oletetaan tunnetuiksi, tietolähteet puolestaan vakiintuneiksi ja kirjattavissa oleviksi. Rekisterinpitäjältä edellytetään sen toiminnan dokumentointia ja säännöksissä vaaditaan suunnitelmallisuutta erityisesti muutosten kohdalla. Rekisterinpitäjä on velvoitettu tuntemaan pitämiensä rekistereiden tietosisältö sekä huolehtimaan tietojen oikeellisuudesta ja asiallisuudesta. Lisäksi etenkin eri rekistereiden sisältämien tietojen yhdistelyyn vaadittiin henkilörekisterilain aikana jopa poikkeuslupia. [Heinonen, 1996; 1997]

Lainsäädännössä on myös lähtökohtaisesti oletettu rekisterinpitäjän ja rekisteröityjen tuntevan toisensa. Samalla rekisteröityjen puolesta on syntynyt luottamus rekisterinpitoa kohtaan ja mahdollisuus saattaa rekisterinpitäjä toiminnastaan vastuuseen. Myös tietojen luovutus rekisteristä on laissa säänneltyä, ja luovutuksen on oletettu toteutuvan asiallisesti. Tietosuojalainsäädännössä rekisteröidyn suhdetta rekisterinpitäjään nähden pidetään alisteisena, ja laissa onkin pyritty huolehtimaan rekisteröidyn oikeuksista. [Heinonen, 1996; 1997]

Verkossa tietojen eri käsittelyvaiheet ovat hajautuneet: tiedot rekisteröidään jossakin, niitä käsitellään toisaalla ja säilytetään muualla. Tietojen hallintakin on näin ollen kompleksisempaa, mikä on omiaan hämärtämään tietojen käsittelyn vastuusuhteita rekisterinpitäjien kesken. [Heinonen, 1998b] Tietoverkossa rekisterinpidon eri vaiheita on vaikea erotella, esimerkiksi tietojen keruu ja niiden luovutus voivat tapahtua käytännössä samanaikaisesti. Verkossa sijaitsevat rekisterit ovat muutenkin joustavia. Muun muassa rekisterin sisältö voi vaihtua jatkuvasti, eikä rekisterinpitäjän voida olettaa täsmällisesti tietävän, mitä tämän ylläpitämään rekisteriin on kulloinkin tallentunut. Tietojen keruukin voi tapahtua jatkuvasti vaihtuvista lähteistä. Verkkopalveluille on ominaista dynaamisuus, räätälöitävyys ja nopea muuttuminen, joten tarkkojen tietosisältöjen määrittely ennalta on vaikeaa. Tietojen paikkansa pitävyyden ja ajantasaisuuden vaatimus on verkkorekisterinpitäjälle melkoinen haaste. [Heinonen, 1996]

Verkkoympäristössä tietojen käsittelytavat ja tekniikat eroavat jo periaatteellisesti keskuskoneperustaisesta toiminnasta erityisesti tietojen haun osalta. Verkkotiedonhaussa eri tietolähteitä ja -varastoja tyypillisesti yhdistellään. Tietolähteitä tärkeämmäksi voi nousta logiikka, muun muassa hakuehdot ja -periaatteet, joilla tiedonhaku suoritetaan. Tiedon sijainninkaan osalta ei fyysisellä ympäristöllä juuri ole merkitystä eikä se aina ole edes tiedossa. Tietoverkossa rekisteröity ja rekisterinpitäjä eivät välttämättä myöskään tunne toisiaan. Näin ollen tietojen rekisteröinti tapahtuu ikään kuin hyväksymällä vallitsevat asiantilat ja käytänteet, eikä rekisterinpidon luottamuksellisuus synny samalla tavoin kuin perinteisessä, tarkoin säännellyssä rekisterinpidossa. Tietoja luovutettaessa ei aina voida olla varmoja siitä, keneltä tiedot ovat peräisin, tai kuka lopultakin tiedot luovuttaa ja kenelle. [Heinonen, 1996; 1997]

Yksityisen henkilön kannalta tarkasteltuna rekisteröidyn rooli on merkittävästi muuttunut. Perinteisessä rekisterinpidossa kansalainen on ollut tiedon kohde, mutta tietoverkossa hän on sähköisen asioinnin käyttäjä [Partanen, 1996]. Erityisesti yksityisten tahojen tarjoamissa verkkopalveluissa käyttäjäksi rekisteröitynyt tosiasiassa osallistuu aktiivisesti itseään koskevaan rekisterinpitoon. Esimerkiksi Alma Media on ottanut kannan, jossa yrityksen palveluiden käyttäjäksi rekisteröityvä velvoitetaan pitämään omat tietonsa ajan tasalla. Käyttäjä sitoutuu tähän velvoitteeseen hyväksymällä palveluiden käyttösopimuksen. Sopimustekstissä[6] todetaan, että monet päätelmät perustuvat käyttäjän antamiin tietoihin, joten on tämän etujen mukaista huolehtia tietojen oikeellisuudesta. Henkilötietolain mukaan vastuu rekisterin tietosisällön oikeellisuudesta, tarpeellisuudesta ja ajantasaisuudesta on kuitenkin rekisterinpitäjällä [HetiL 29 §]. Voisiko rekisteröidyn ja rekisterinpitäjän keskinäisellä sopimuksella ohittaa laintasoista säännöstä? Oikeuskäytännössä sellaista sopimusta ei välttämättä pidetä pätevänä, jossa lailla suojeltava osapuoli luopuu lakisääteisistä oikeuksistaan. Mikäli vastuusuhteista syntyisi kiistaa, lopullinen ratkaisu luultavasti selviäisi vasta oikeusistuimen päätöksen myötä.

5.2. Tietojen varastointi ja louhinta

Tietovarastointi (*data warehousing*) on menetelmä, jolla tietoja kerätään, jalostetaan ja yhdistellään organisaation operatiivisista tietokannoista. Tietoa kertyy esimerkiksi yrityksen toiminnan tuloksena, sillä asiakaspalvelun, logistiikan, laskutuksen, perinnän, markkinatutkimuksen, osto- ja maksutapahtumien sekä tilausten ja palautusten prosessit tuottavat tietokantoihin tallennettavia tapahtumatietoja [Klemetti, 1998]. Kehittyneelle tietojenkäsittelylle on ominaista, että myös aiemmin täysin käyttökelvottomina pidetyt tiedonmuruset ovat nykyisin keräämisen arvoisia. Verkkoympäristössä jokainen hiiren liikahdus on rekisteröitävissä. Koska tiedon varastoinnin ja analysoinnin tekniikat edistyvät jatkuvasti, kannattaa verkon tapahtumatietoja kerätä jopa tulevia, vielä tuntematomia käsittelytarpeita varten. [Heinonen, 1998b]

---

[6] ks. esimerkiksi http://guard.almamedia.fi/aa/perustiedot.html?SERVICE_ID=20, linkki "käyttösopimuksen"

Operatiivisiin tietokantoihin tallennettu tapahtumatieto on yksinään hyödytöntä ja raakaa dataa. Se on kuitenkin jalostettavissa hyödylliseksi informaatioksi. [Klemetti, 1998] Tapahtumatietojen analysoinnissa käytetään muun muassa tiedon louhintaa (*data mining*). Louhintaprosessissa suurista tietomääristä etsitään syy—seuraus-suhteita. [Heinonen, 2003] Esimerkiksi ostoskorin analysoinnilla saadaan selville säännönmukaisuuksia, luokitteluja, poikkeuksia ja trendejä. Asiakkaan käyttäytymisen tutkimisella selvitetään tyypillinen asiakas ja hänen käyttäytymisensä kussakin tilanteessa. Riskien hallinnassa analysointiperusteina ovat muun muassa maksukyky, maksutapa ja luotettavuus. Tiedon louhinta mahdollistaa myös aiemmin tuntemattomien kytkentöjen löytymisen. Louhinnalla voidaan siksi saada vastauksia kysymyksiin, joita menetelmän soveltaja ei ole tullut edes ajatelleeksi. Mikäli analysoijalla ei ole selkeää käsitystä siitä, mitä hän aineistosta haluaisi tietää, voi menetelmä tuottaa yksityisyyttä vaarantavia tietosisältöjä. [Heinonen, 1998a]

Tietovarastoinnin mahdollistamaan mallintamis-, raportointi- ja analysointitekniikkaan voidaan yhdistää myös ulkopuolisia tietolähteitä. Useista tietolähteistä kootulle tiedolle saattaa kuitenkin tulla eheysongelmia, sillä lähtötiedot voivat olla eri tavoin johdettuja, korjailtuja tai puutteellisia. Jotta hajautetuista tietolähteistä saataisiin ristiriidatonta tietoa, tulee toiminnan perustua yhteiseen tietovarastoarkkitehtuuriin ja tietomalliin. Tietosuojan kannalta tietovarastoinnin kriittinen vaihe on metadatan generointi. Metadatalla tiedot ovat yhtenäistettävissä myös operatiivisen tiedon muuttuessa. Heinonen [1998a] toteaakin, että tietovaraston tietosuoja voi olla vain niin hyvä kuin sen metadatan tietosuoja on.

5.3. Henkilötietojen kaupallistuminen

Tietoteknisen kehityksen myötä henkilötiedoille on yllättäen syntynyt markkina-arvo. Aiemmin yritykset miettivät keinoja, joilla saisivat kerrottua asiakkaille mahdollisimman paljon itsestään. Nykyisin kehitys kulkee toiseen suuntaan yritysten pyrkiessä saamaan tietoja asiakkaistaan. Tätä varten kehitellään erilaisia järjestelmiä: verkkopalveluja, kanta-asiakaskortteja ja nimellisiä etuisuuksia, joita vastaan henkilötiedot on luovutettava. [Heinonen, 1998a; Järvinen, 2002] Tietojen hankintaan on kuitenkin helpompikin tapa, sillä voihan niitä myös ostaa valmiiksi kerättyinä.

Julkisen sektorin rekisterinpitäjillä on usein jokin lakisääteinen tehtävä ylläpitämiensä rekisteritietojen keräämiseen. Näin ollen julkinen valta velvoittaa ja jopa pakottaa kansalaiset antamaan tietoja itsestään. Koko väestön kattavan ja systemaattisesti kerätyn tietosisältönsä takia lakisääteisin perustein kerätty rekisteritieto on ruvennut kiinnostamaan myös kaupallisia tahoja. Julkisten tahojen ylläpitämät rekisterit ovat erityisen haluttuja laadukkuutensa ja luotettavuutensa vuoksi. Julkinen sektori on puolestaan huomannut hallinnoimansa tiedon kaupallisen arvon. Näin ollen paine on kasvanut näidenkin tietojen käyttämiseksi kaupallisiin tarkoituksiin. [Heinonen, 1998b; Mantere, 1998]

Uuden-Seelannin yksityisyyskomissaari Bruce Slane huomauttaa, ettei julkisten ylläpitäjien rekistereiden massaluovutuksia tulisi vaatia tiedon vapaan liikkuvuuden varjolla. Tiedon julkisuuden ja vapaan liikkuvuuden tavoitteena on lisätä hallinnollisen menettelyn avoimuutta ja luottamusta viranomaistoimintaa kohtaan sekä parantaa kansalaisten osallistumismahdollisuuksia. Tietojen luovutus kaupallisiin tarkoituksiin ei ole sopusoinnussa näiden tavoitteiden kanssa. Hallinnollisten rekistereiden kaupallinen käyttö saattaa lopulta haitata rekistereiden käyttötarkoitusta ja luotettavuutta. [Mantere, 1998] Virtasen [2002] mielestä tahoilta, joilla on lakisääteinen oikeus henkilötietojen keräämiseen, tulisikin kieltää henkilötietoihin liittyvä liiketoiminta.

5.4. Digitaalisen persoonan profilointi

Heinonen [2001a] puhuu digitaalisesta persoonasta, jolla hän tarkoittaa "henkilöä koskevien tietojen avulla rakennettua kokonaisuutta." Tätä rakennelmaa käytetään henkilön edustajana esimerkiksi kansalaisen tai kuluttajan rooleissa. Käsitteessä on oleellista, ettei henkilö rakenna digitaalista persoonaansa itse, vaan se tehdään esimerkiksi viranomaisten toimesta.

Digitaalisen persoonan rakentaminen ja ylläpito perustuu tietoverkoissa tapahtuvaan vuorovaikutteiseen toimintaan. Henkilön kuvaus saadaan aikaan keräämällä yksilöstä jäsenneltyä, tapahtumiin perustuvaa tietoa. Saatu tulos on yksilön malli ja samalla yksinkertaistettu todellisuuden kuvaus. Digitaalisen personoinnin puutteena on, ettei yksilöä käsitellä kokonaisuutena — sen sijaan hyvin yksinkertainen tietojoukko katsotaan riittäväksi edustamaan henkilön merkittävimpiä piirteitä ja ominaisuuksia. Esimerkki digitaalista persoonaa kuvaavasta tiedosta on vaikkapa ajankohta, jolloin henkilö tietoverkossa asioi. Samalla yksilöllä voi tyypillisesti olla useita digitaalisia persoonia. [Heinonen, 2001a]

Profilointitekniikassa määritellään ensin halutut luokat ja sitten piirteet, jotka kuvaavat luokan profiilia. Profiilia rakennetaan analysoimalla niitä tietovarastoja, joihin profiloitavat kuuluvat muun muassa eristämällä heidän yhteiset piirteensä. Lopuksi etsitään tietoja henkilöistä, jotka sopivat haluttuihin piirteisiin mahdollisimman tarkasti. Profilointi voi perustua organisaation jo omistamaan tietoon, mutta toimintaan käytetään yhä enemmän varta vasten kerättyjä tietoja. Staattisen tiedon lisäksi hyödynnetään esimerkiksi toimenpiteistä ja tapahtumista syntyvää tietovirtaa. [Heinonen, 2001a]

Henkilökohtaiseksi profiloinniksi nimitetään toimintaa, jossa kerätään yksilöä koskevia tietoja ja verrataan niitä laajempiin demografisiin tietoihin. Näin toimitaan erityisesti markkinoinnin kohdentamiseksi ja verkkosivustojen personoimiseksi. Henkilökohtaisen profiloinnin vastakohtana on abstrakti profilointi, jossa seulotaan suuria tietomääriä esimerkiksi rikollisten löytämiseksi. [Heinonen, 2001a]

Profiloitavien piirteet johdetaan menneistä kokemuksista, joista osa on epätarkkaa tietoa, kuten oletuksia, näkemyksiä ja todennäköisyyksiä. Varsinkin erilaisista tietokannoista yhdistellyn tiedon pohjalta saadaan aikaiseksi yksityiskohtainen ja laaja, mutta

pirstaleinen yksilön digitaalinen kuvaus. Kun profiloitavalla henkilöllä ei ole käytännön mahdollisuutta vaikuttaa hänestä luotavan kuvan kokoamiseen, on profiili aina vinoutunut palvelemaan kokoajan tarkoitusperiä. Heinosen [2001a] mukaan erityisesti julkisen vallan harjoittama profilointi uhkaa yksilön oikeuksia. Mikäli profilointia käytetään ennakoivana toimintana tunnistamaan ja julistamaan henkilöitä syyllisiksi ennen asian tutkimista, edustaa profilointi ennalta tuomitsemista. Tällöin esimerkiksi luottotoiminnassa ja verotuksessa luodaan edellytyksiä ennakoivaan syrjintään jälkikäteen tapahtuvan tuomitsemisen sijasta.

Profiloinnille on ominaista, että henkilöstä vastaanotetaan vain profiloijan tavoitteita vahvistava tieto, vaikka monipuolisempaakin olisi tarjolla. Näin profiili piirtyy valittujen kriteerien perusteella erilaiseksi eri tilanteita ja tarkoituksia varten. Toinen profiloinnille tyypillinen ominaisuus on sen tarkoituksellinen salaaminen tai toiminta muutoin profiloitavan tietämättä. Profilointia käyttävät organisaatiot pitävät toimintaa kilpailu- tai turvallisuustekijänä, jonka hyödyt saattavat vaarantua, mikäli menettely olisi julkista. [Heinonen, 2001a]

Profiloinnilla on hyvät ja huonot puolensa. Luottokortin käytöstä luotu profiili ja kortin käytön seuranta edesauttaa varastetun luottokortin pikaista sulkemista, sillä profiilista poikkeavaksi muuttunut kortin käyttö hälyttää valvovan järjestelmän. Vastaavasti normaalistikin hulppeasti korttiaan käyttelevä voi profiloitua pankin ei-toivottujen asiakkaiden listalle. Mainonnassa profiloinnilla voidaan välttää mainosten lähettäminen niille kuluttajille, jotka eivät kyseisiä tuotteita halua. Toisaalta entistä tarkemmin kohdennetuilla mainoksilla manipuloidaan kuluttajia. Heinonen [2001a] huomauttaa, että mitä yksityiskohtaisempi, kattavampi ja ajan tasalla olevampi profiili on, sitä enemmän profilointi muistuttaa aivopesua.

Profilointitarkoituksiin kerätään tietoa muun muassa henkilön kyvyistä, taipumuksista ja tavoista [Heinonen, 2001a]. Tällaisen tiedon kerääminen muodostuu helposti lainvastaiseksi. Henkilötietolaissa arkaluonteiseksi määritellyn tiedon käsittely on kielletty. Esimerkkejä lain 11. §:ssä arkaluonteiseksi määritellystä tiedosta ovat kuvaukset rodusta tai etnisestä alkuperästä, yhteiskunnallisesta, poliittisesta, tai uskonnollisesta vakaumuksesta, ammattiliittoon kuulumisesta, seksuaalista suuntautumisesta tai terveydentilasta. Poikkeuksia käsittelykieltoon tuovat muun muassa tilanteet, joissa tietojen käsittelystä on säädetty laissa, rekisteröity on antanut tietojen käsittelyyn nimenomaisen suostumuksensa tai itse saattanut tiedon vakaumuksestaan tai ammattiliittoon kuulumisestaan julkiseksi.

Heinosen [2001a] mukaan profilointi puuttuu aina yksityisyyteen ja sisältää huomattavia yksityisyyden loukkausten ja muun rikollisen toiminnan mahdollisuuksia. Yhdessä tietojen yhdistelyn kanssa profilointi mahdollistaa massatietovalvonnan ja tehokkaan kansalaisten kontrollin viranomaistoiminnassa — saatamme pian huomata elävämme tietoyhteiskunnan lisäksi valvontayhteiskunnassa. Lisäksi ihmisten tapojen ja liikkumisen kasvanut näkyvyys helpottaa myös identiteetin väärinkäyttäjien toimia, ja

Internet on digitaalisen persoonan varkaiden paratiisi. [Heinonen, 2001a] Sähköisen viestinnän tietosuojalain valmistelutöissä profilointiin on kiinnitetty huomiota. Lainsäätäjäkin on havainnut Internet-palvelujen tarjoajien olevan keskeisessä asemassa käyttäjien kulutustottumuksia ja elämäntapoja koskevan tiedon käytön kannalta. Vaikka käyttäjäprofiilien luominen on markkinoinnin näkökulmasta houkuttelevaa, ilman profiloidun suostumusta tapahtuvaa tietojen käyttöä ja luovuttamista on syytä rajoittaa. [HE 125/2003]

Yksityisyyden turvaamiseksi on siis syntynyt kattavampien ja selkeämpien säännösten tarve sähköiseen viestintään liittyvien tietojen käsittelystä ja luovuttamisesta. Mikäli käyttäjän tietokoneelle tallennetusta evästeestä saatavia tietoja yhdistetään esimerkiksi palvelun käyttäjäksi rekisteröitymisen yhteydessä annettaviin tietoihin, on käyttäjien profiloiminen teknisesti mahdollista. [HE 125/2003] Sähköisen viestinnän tietosuojalakiin on lisätty säännökset sekä evästeiden että tunnistamistietojen käsittelystä [SVTSL 7 § ja 3.s luku]. Laki ei kuitenkaan varsinaisesti kiellä profilointia.

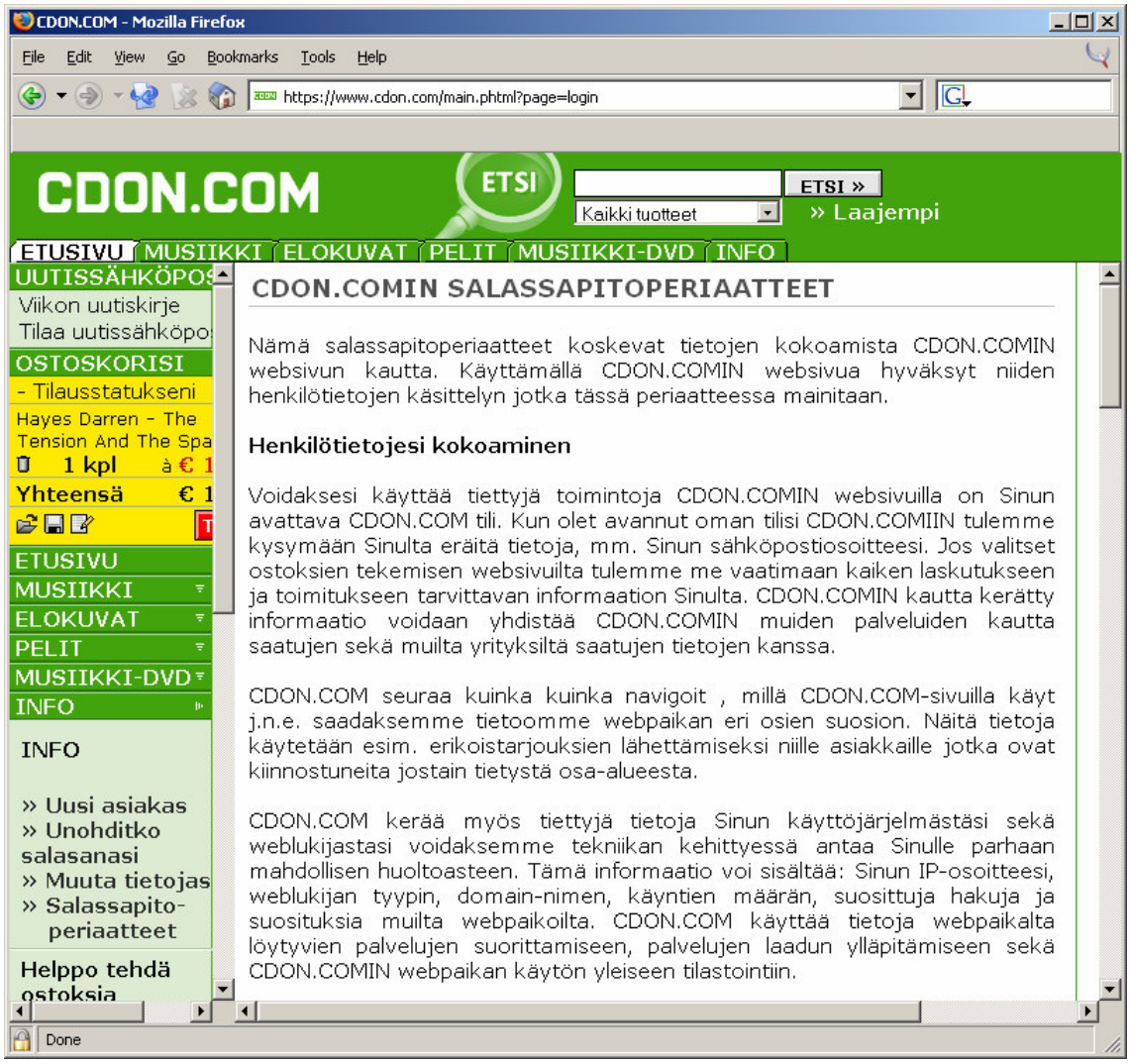
Henkilötietolakikaan ei ota kantaa profilointiin. Heinosen [2001a] mukaan se sallitaan, mikäli profilointi on rekisterinpitäjän toiminnan kannalta perusteltua. Niinpä laittoman ja laillisen profiloinnin erottelu on hankalaa. Heinonen arvioi, että toimintaa voisivat lainsäädännön lisäksi rajoittaa julkinen mielipide ja huoli profiloinnin seurauksista. Tosin keskustelu sopivasta tai sopimattomasta profiloinnista on tähän mennessä ollut olematonta, joten lupaus profiloinnin harjoittamattomuudesta ei toistaiseksi ole toiminut yritysmaailmassa kilpailuvalttina.

5.5. Profiloinnin seurauksia

Äärimmillään profilointi johtaa kuluttaja-apartheidiin. Kun asiakkaat tunnistetaan, heidät jaetaan eri tavoin kohdeltaviin ryhmiin esimerkiksi sen mukaan, miten merkittävä ryhmä kaupallisesti on. Toiminnan englanninkielinen nimitys on *customer relations management*, *CRM*. Palvelut, joihin on sovellettu CRM:ää, hinnoitellaan eri henkilöille eri tavoin, ja esimerkiksi pankin lainaehdot muuttuvat asiakasryhmän mukaisesti. Huonoiksi koetuille asiakkaille saatetaan jopa antaa tarkoituksellisesti huonoa palvelua siinä toivossa, että he vaihtaisivat asiakassuhteensa muualle. [Järvinen, 2002]

CRM soveltuu hyvin verkkopalveluihin, sillä IP-osoitteen, evästeen, asiakasnumeron tai muun tunnisteen avulla on helppo määritellä, mihin ryhmään asiakas kuuluu. Esimerkiksi palvelun lomakekentät voivat vaihtua sen mukaan, miten yhteydenottaja on segmentoitu. Kuten profilointia yleensäkin, myös CRM:ää käytetään asiakkaiden tietämättä. Vaikka menetelmä ei olekaan erehtymätön, muutamalla virhearvioinnilla ei kokonaistoiminnan kannalta ole merkitystä. [Järvinen, 2002] Lopulta asiakkaitten ei ole mahdollista tehdä tietoisia valintoja, sillä segmentointi rajoittaa tiedon saatavuutta. Kuluttajat eivät myöskään ole enää yhdenvertaisia keskenään. Samalla kun markkinoijien tietämys kuluttajista kasvaa, lisääntyy myös markkinoivien tahojen valta. [Heinonen, 2001a]

Profiloinnin yleistyttyä myös kaupanteko on muuttanut luonnettaan. Verkkokaupassa on yhä harvemmin mahdollista pelkästään tilata ja maksaa tuotteita. Sen sijaan palvelun käyttäjän on luovutettava itseään kuvaavia tietoja, joita ei tarvittaisi varsinaisen ostotapahtuman hoitamiseen. Tietoja vaaditaan tilauksen yhteydessä joko suoraan tai niiden kysyminen naamioidaan "lukijaklubiin" liittymiseksi tai vastaavaksi sijaistoiminnoksi. Kehittyneiden tiedonjalostustekniikoiden mahdollistaessa kuluttajien mieltymysten ja verkkosivuston käyttötietojen yhdistelyn harva verkkokauppias tyytyy perinteiseen kaupantekoon. Esimerkiksi CDON.COM-verkkokaupasta oli aiemmin mahdollista tilata tuotteita pelkästään nimi- ja osoitetiedoin. Nykyisin palvelu kerää tilauksen yhteydessä kuluttajista yksityiskohtaisia tietoja, jotka lisäksi yhdistetään palvelun käyttämistietoihin (Kuva 7).



Kuva 7. Verkkokauppa CDON.COM yhdistelee tiedot palvelun käytöstä asiakkaan henkilötietoihin.

Vaikka asiakas kieltäisi itseensä kohdistuvan suoramarkkinoinnin, on tämän luovutettava tietojaan profilointitarkoituksiin ja siten osallistuttava markkinoiden kehittämiseen.

Yhä harvempi verkko-ostos on mahdollinen ilman ylimääräisten tietojen luovuttamista, joten kuluttajalla ei ole todellisia vaihtoehtoja. Mikäli tämä ei halua luovuttaa tietojaan, on hankinnat tehtävä muualta.

Verkkosivustojen ostotapahtumien tarkka seuraaminen ja analysointi mahdollistaa siirtymisen kohdistettuun vuorovaikutteiseen viestintään eli täsmämarkkinointiin (*one-to-one*). Täsmämarkkinointi onnistuu sitä paremmin, mitä intensiivisempi vuorovaikutus asiakkaan ja yrityksen välillä on. Vuorovaikutusta siis tehostetaan kyselyillä, kilpailuilla ja tarjouksilla. Kaupallisen yrityksen tavoitteena on, että asiakas sitoutuisi palveluun, jotta hän myös ylläpitäisi ja päivittäisi omia tietojaan. Tietovarastoinnin ja louhinnan ansiosta jokaista asiakasta voidaan kohdella aidosti yksilönä. [Heinonen, 1998a] Kaiken lisäksi täsmämarkkinointi on perinteisiin menetelmiin verrattuna edullista, joten kustannukset, jotka aiemmin käytettiin mainostilan ja -ajan ostamiseen, voidaan kohdentaa toisaalle [Järvinen, 2002].

Profiloinnin kielteisinä vaikutuksina pidetään markkinoinnin valikoivuuden ja syrjinnän lisäksi kuluttajien manipulointia. Uudenlainen verkkomarkkinointi edesauttaa tarkan asiakasprofiilin rakentamista käyttäjän kulkureittejä seuraamalla. Markkinointiviestien lähetyksen jälkeen tulos on heti mitattavissa. Profiilia voidaan hioa ja tarkentaa entisestään esimerkiksi seuraamalla, minkä linkkien kautta kukin asiakas reagoi tai vastasi viestiin. Heinonen [2001a] huomauttaa, että profiloinnilla on kyky parantaa viestinnän vaikutuksia sen kohderyhmään. Profiili mahdollistaa jopa asiakkaiden käyttäytymisen ennakoinnin. Tietosuojalainsäädännön kanta on selvä: mikäli yksilön käyttäytymistä voidaan henkilötietojen avulla ohjata tietyllä tavalla, tapahtuu yksityisyyden suojan loukkaus.

5.6. Kasvaako rekisteröidyn vastuu?

Yksityisyyden sääntelyn toteutus voidaan jakaa kahteen tyyppiin, lainsäädäntöön ja markkinoihin perustuvaan itsesäätelyyn [Heinonen, 2001a]. Lainsäädännössä rekisteröidyn asemaa pidetään heikompana rekisterinpitäjään nähden, joten laki turvaa ennen kaikkea rekisteröidyn oikeuksia [Heinonen, 1996]. Itsesäätelyn näkökulmassa markkinat osoittavat vallitsevat käytännöt, ja yritysten on oma-aloitteisesti otettava kuluttajien mielipiteet huomioon, sillä tyytymätön asiakas on menetetty asiakas. Itsesäätelymallissa yksilöön suhtaudutaankin aloitteellisena ja valintoja tekevänä tahona, jolla on valta vaikuttaa aktiivisesti henkilötietojensa käsittelyyn [Heinonen, 2001a]. Eurooppalainen tietosuoja on perinteisesti lakisääteistä, kun esimerkiksi Yhdysvalloissa käytetään pääasiassa markkinaperustaista itsesäätelymallia.

Itsesäätelymalli näyttäisi monelta osin sopivan verkkoympäristöön lainsäädäntöä paremmin. Verkkoasioinnissa aloitteentekijän asema voi olla rekisteröitävällä, ja jopa tietojen ylläpito sekä päivittäminen saattaa olla rekisterinpitäjän asemesta rekisteröidyn vastuulla. Mikäli päätös tietojen rekisteröinnistä on rekisteröityvällä, voitaisiin hänelle Heinosen [1996] mukaan sälyttää myös vastuuta normaalia enemmän. Jos rekisteröity

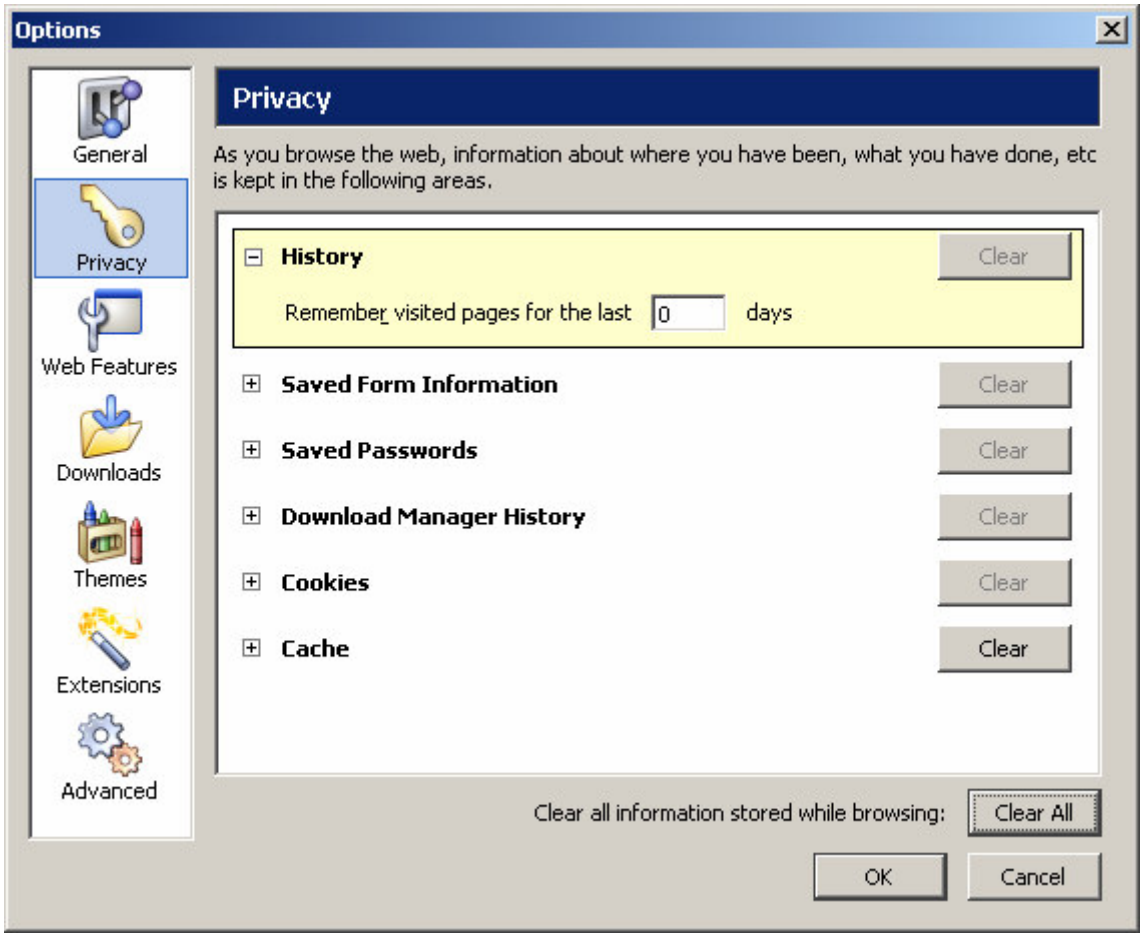
osallistuu omien tietojensa käsittelyyn, saattaisi tietosuojan sääntelyn merkitys vähetä, ja kansalaisten käsitykset hyvästä ja hyväksyttävästä rekisterinpidosta tulisivat viranomaisarvioita tärkeämmiksi.

Heinonen [1996] huomauttaa, ettei verkkoympäristössä ehkä ole järkevää tai edes mahdollista säädellä täsmällisesti, miten, missä, millä tekniikalla tai kenen toimesta mitäkin tietoja käsitellään. Yksityiskohtaisen sääntelyn haittapuolena on se, että säännökset vanhenevat nopeasti teknisen kehityksen rinnalla, mistä puolestaan seuraa sekä tulkinta- että valvontaongelmia. Erityisen vaikeita valvottavia ovat verkossa tahattomasti jätettyjen jälkien rekisteröinnit. Tämä johtaa Heinosen kysymään, pitäisikö rekisteröidyn kantaa keskeinen vastuu myös sähköisten jalanjälkien rekisteröimisestä? Myös Järvisen [2002] mielestä jokaisen Internetin käyttäjän tulisi osata välttää tahaton sähköisten jalanjälkien jättäminen. Mikäli viranomaisten holhoaminen vähenee, rekisteröidyn valmius toimia oikeuksiensa puolesta saa yhä suuremman painoarvon. Heinonen [1996] ehdottaakin, että tietosuojan taitaminen olisi jatkossa sovitettava rekisteröidyn kykyyn jättää jälkiä itsestään tietoisesti.

Heinosen ja Järvisen vaatimukset vaikuttavat liian optimistisilta ja hyvin omaan asiaansa perehtyneiden ihmisten tyypillisiltä kommenteilta. Tietoyhteiskuntakehitys on vasta alullaan, eikä kansalaisilla ole vielä riittävää tietosuojaosaamista tietotekniikan hyvästä hallinnasta puhumattakaan. Asiaa voi verrata tavallisten tietokoneen käyttäjien virusten torjuntakykyyn. Virukset leviävät, sillä kaikesta saatavilla olevasta ohjeistuksesta huolimatta käyttäjille on epäselvää, kuinka virusten ja muiden haittaohjelmien kanssa tulisi toimia. Niinpä sähköisen viestinnän tietosuojalakiin on otettu säännökset, joiden mukaan teleyritys tai yhteisötilaaja voi poistaa viesteistä sekä haittaohjelmat että suurina määrinä lähetetyt automaattiset markkinointiviestit [19 § ja 20 §; HE 125/2003]. Poistaminen on mahdollista, jos se on välttämätöntä sähköisen viestinnän toimintakyvyn turvaamiseksi. Lain valmistelutöissä on todettu, että sähköpostiviestien tarkastamisen tulee olla mahdollista jopa ilman viestin vastaanottajan suostumusta — muutoin sähköiset viestintäpalvelut voisivat menettää toimintakykynsä. [HE 125/2003] Henkilötietojen käsittelyn ja yksityisyyden suojaa tulisi tällä hetkellä vastaavasti pikemminkin automatisoida rekisteröidyille asetettavien velvoitteiden sijasta.

Mikäli käyttäjiltä vaadittaisiin vastuunottoa sähköisten jalanjälkien jättämisestä, tulisi teknologiaa kehittää suuntaan, jossa jälkien hävittäminen tai peittäminen olisi mahdollisimman yksinkertaista. Nykyisissä selainohjelmissa esimerkiksi välimuistin tyhjentäminen ei onnistu ilman selainasetusten tuntemusta. Lisäksi historiatietojen hävittämisen toteutus ja toimintojen nimeämiskäytäntö poikkeaa eri selainvalmistajien kesken melko paljon. Toimintoja olisi kuitenkin mahdollista yhdenmukaistaa ja selkeyttää. Esimerkiksi Mozilla Firefox -ohjelman dialogissa selaimeen jäävät jäljet voidaan hävittää yhdellä painalluksella (Kuva 8). Jotta käyttäjän ei tarvitsisi haeskella jälkien hävittämistoimintoja eri tavoin toteutettujen dialogien viidakosta, voitaisiin selainten painikeriville lisätä painike, joka tyhjentäisi kerralla kaikki liikennöinnistä jäävät jäljet.

Verkkoliikennöinnin salauspalvelujen kehityttyä nykyistä paremmiksi, voitaisiin selaimiin lisätä vastaavanlainen painike myös anonyymiä Internet-sivujen selausta varten.



Kuva 8. Firefox-selaimessa on selkeä dialogi, jossa selaimeen jäävien jälkien hävittäminen onnistuu yhdellä painalluksella (*Clear all*).

6. Sähköiset jalanjäljet

Internetin käytön alkuaikoina vallinnut käsitys verkossa liikkumisen anonyymiudesta on osoittautunut virheelliseksi. Verkkoliikennöinti jättää jäljet omaan työasemaan, operaattoreiden tiedostoihin sekä verkkosivustoihin, joilla käyttäjä on vieraillut. Verkossa liikkumisesta jääviä tietoja kutsutaan sähköisiksi jalanjäljiksi, joihin luetaan sähköpostiosoitteiden ja käyttäjätunnusten lisäksi muun muassa IP-osoite (*internet protocol*) sekä palomuurin (*firewall*) ja välityspalvelimen (*proxy*) osoitteet.

Kuten järkevää onkin, lainsäätäjä ei ole erikseen luetellut, millaisia tietoja voidaan pitää henkilötietoina. Henkilötietolain määritelmän mukaan henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä. Edellytyksenä on, että merkinnät voidaan tunnistaa tiettyä henkilöä tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. [HetiL 3 §] Käyttäjätunnusten, opiskelijanumeroitten ja muitten vastaavien merkintöjen osalta määritelmää tulkitaan seuraavasti: mikäli henkilö on mahdollista merkinnän perusteella tunnistaa esimerkiksi eri tiedostoja yhdistelemällä, on merkintä henkilötieto. Henkilötietojen keräämisenä on puolestaan henkilörekisterilain valmistelutöissä pidetty myös rekisterinpitäjän toiminnan seurauksena kerääntyviä henkilötietoja. [HE 49/1986] Tällaisia ovat esimerkiksi operaattoreiden loki- ja käyttötiedostot.

Osa sähköisistä jalanjäljistä ei yksinään voi paljastaa käyttäjää henkilötasolle saakka. Esimerkiksi pelkän IP-osoitteen perusteella on lähes mahdotonta selvittää koneen käyttäjän henkilöllisyyttä, vaikka osoite onkin tärkeä jälkien lähde. Yhteisötilaajan IP-osoite voidaan jäljittää organisaatioon asti, mistä eteenpäin tulisi päästä käsiksi yrityksen tai laitoksen sisäisiin jäljitystietoihin. Näihin ulkopuolisilla ei ole luvallista pääsyä. Modeeminkäyttäjän IP-osoite on puolestaan vaihtuva, jolloin osoitteen omistajan tuntee ainoastaan operaattori. [Järvinen, 2002]

6.1. Loki-, tunnistamis- ja tapahtumatiedot

Myös lokitiedoista muodostuu henkilörekisteri, mikäli tiedot sisältävät merkintöjä, joista henkilö on tunnistettavissa. Tietosuojaviranomaisten ohjeissa lokijärjestelmällä tarkoitetaan tietojärjestelmää, jonka tarkoituksena on suojata rekisteröityjä tietoja ja rekisteröidyn yksityisyyttä. Lokijärjestelmällä rekisterinpitäjä siis vastaa henkilötietojen käsittelyn lainmukaisuudesta ja kontrolloi, että rekisteröityjen henkilötietojen käsittely on annettujen ehtojen ja määräysten mukaista. [Käyttäjälokin tietojen..., 2003] Järjestelmien oikean ja asianmukaisen käytön lisäksi lokilla varmistetaan tietojen käsittelijöiden valtuudet ja oikeudet. Turvallisuustekijöiden lisäksi ylläpitäjä voi seurata lokilla tietojärjestelmän tehokkuutta. Lokitiedoilla tietojenkäsittelystä saadaan kontrolloitua, sillä loki kertoo, mitä on tapahtunut, milloin, millä tavoin ja kenen toimesta. [Heinonen, 2003]

Heinonen [2003] huomauttaa, ettei organisaation ylläpitohenkilöstökään useimmiten tiedä toimivaltansa rajoja ja lokitietojen käyttöoikeuksia. Osa ongelmaa on tietojen käsittelyn asianmukaisuuden valvonnan vaikeus. Rikosepäilyn sattuessa lokien ylläpidosta vastaavien ei tule leikkiä salapoliisia, sillä rikosten tutkinta kuuluu viranomaisille. Ylläpidon lisäksi organisaation johto saisi Heinosen [2003] mielestä olla tietoisempaa ja paremmassa valmiudessa lokitietojen käsittelyn suhteen.

Operaattori saattaa käyttää välityspalvelinta, jolloin sen lokeihin tallentuu tieto jokaisesta Internet-verkosta haetusta sivusta. Välityspalvelin ei ole enää nykyisin ohitettavissa eikä palvelin myöskään paljastu käyttäjälle. [Järvinen, 2002] Vastikään voimaan astuneessa sähköisen viestinnän tietosuojalaissa tällaisia sähköisestä viestinnästä syntyviä tietoja kutsutaan tunnistamistiedoiksi. Laissa on selkeytetty tunnistamistietojen käsittelysääntöjä, ja tiedot ovat pääsääntöisesti luottamuksellisia. Uuden lain myötä tunnistamistietojen käsittelyoikeuksia ja -velvollisuuksia laajennettiin koskemaan myös yhteisötilaajia. Esimerkkejä yhteisötilaajista ovat elinkeinoyritykset ja yliopistot. [HE 125/2003]

Tunnistamistiedolla tarkoitetaan siis käyttäjään yhdistettävissä olevaa tietoa, jota käsitellään viestintäverkoissa esimerkiksi viestien siirtämiseksi. Tunnistamistiedot voivat viitata muun muassa viestinnän kestoon, ajankohtaan tai vastaanottajan päätelaitteen sijaintiin. [HE 125/2003] Sähköisen viestinnän tietosuojalaissa tunnistamistietojen käyttö rajoitetaan vain laissa mainittuihin tarkoituksiin. Käytön rajoittamisen lisäksi säännöksillä informoidaan tunnistamistietojen käsittelijää siitä, että kaikissa tietojen käsittelytilanteissa käsittelyn perusteiden on löydyttävä laista — muihin tarkoituksiin tietoja ei saa käyttää. Käsittelyn jälkeen tunnistamistiedot on hävitettävä, mutta niiden käsittelystä on tallennettava yksityiskohtaiset tapahtumatiedot. Tapahtumatiedoista on käytävä ilmi tunnistamistietojen käsittelyn ajankohta, kesto ja käsittelijä. Tapahtumatietoja on säilytettävä kaksi vuotta niiden tallentamisajankohdasta. [SVTSL 3.s luku]

Verkkoliikennöinnin lisäksi tietoa voidaan koota hiiren ja näppäimistön käytöstä. Internet-sivustojen vuorovaikutteisten komponenttien, kuten esimerkiksi valikoiden ja ikkunoiden, käyttö on rekisteröitävissä. Tietoja voidaan kerätä sekä kaupallisiin että valvontatarkoituksiin. Kun kerätyt tiedot ovat identifioitavissa eli yhdistettävissä tiettyyn henkilöön, voidaan niiden perusteella esimerkiksi analysoida asiakkaan käyttäytymistä tiedon louhinta- ja profilointimenetelmin. Esimerkiksi pankit ja kaupat ovat erityisen kiinnostuneita osto- ja maksutapahtumista asiakkaittensa profilointitarkoituksessa. [Heinonen, 2003]

6.2. Evästeet

Evästeet ovat tilaobjekteja, jotka kulkevat www-sivujen mukana HTTP-protokollan (*hypertext transfer protocol*) välityksellä. Palvelimen ohjelma lähettää evästeen, jonka käyttäjän selain ottaa vastaan. Evästeitä on kahden tyyppisiä, istuntokohtaisia (*per session, session cookies*) ja pysyviä (*persistent*). Istuntokohtaiset evästeet säilyvät muistis-

sa selaimen aukiolon ajan, mutta tuhoutuvat, kun selain suljetaan. Pysyvät evästeet sen sijaan tallentuvat tekstitiedostoina työasemaan ja säilyvät käyttäjän koneessa, kunnes samalta koneelta otetaan uudelleen yhteyttä evästeen asettaneeseen palvelimeen. Tällöin selain palauttaa evästeen palvelimelle, joka näin tunnistaa käyttäjän vierailleen kyseisellä sivulla jo aiemmin. Evästeet pystyvät erittelemään saman koneen eri käyttäjät, mikäli käyttöjärjestelmänä on Windows, käyttäjällä on oma käyttäjätunnus ja selaimena Internet Explorer. Muussa tapauksessa evästeet tallentuvat ainoastaan konekohtaisesti. Useimmiten evästeille on asetettu jokin vanhenemisaika, jonka jälkeen niitä ei enää palauteta. [Järvinen, 2002]

Evästeiden kehittämisen alkuperäinen tarkoitus on ollut verkkopalvelujen toimivuuden parantaminen. Tilatonta (*stateless*) HTTP-protokollaa käytettäessä käyttäjää ei voida yksilöidä eri sivuhakujen välillä. Tilattomassa protokollassa palvelin joutuu käsittelemään jokaisen www-sivun hakupyynnön erikseen, eikä peräkkäisilläkään hakupyynnöillä ole keskenään mitään yhteyttä. Käyttäjän tiedot voitaisiin teoriassa sitoa IP-osoitteeseen, mutta saman osoitteen takana saattaa olla useita käyttäjiä, ja osoite voi myös vaihtua eri yhteyskerroilla. [Järvinen, 2002]

Eväste siis tunnistaa verkkopalvelun käyttäjän eri sivuhakujen ja käyntikertojen välillä. Tunnistaminen on tarpeen erityisesti verkkokauppojen ostoskorien ylläpidossa, mutta tekniikalla on käyttöä missä tahansa verkkopalvelussa, jossa käyttäjän antamien tietojen tulee olla saatavilla koko istunnon ajan. Mikäli käyttäjä on luovuttanut verkkopalvelulle omia henkilötietojaan, ne voidaan yhdistää samaan henkilöön eri käyttökertojen välillä. Pysyvillä evästeillä esimerkiksi luodaan henkilökohtaisen palvelun vaikutelma personoimalla sivusto asiakkaan mieltymysten mukaiseksi. Evästeeseen tallennetut preferenssit voivat olla yhtä hyvin käyttäjän itsensä antamia henkilö- ja muita tietoja kuin käyttäjän tietämättä tehtyyn profilointiin perustuvia vihjeitä.

Sähköisen viestinnän tietosuojalain 7. §:ssä säädetään palvelun käyttöä kuvaavien tietojen tallentamisesta käyttäjän päätelaitteelle. Pykälässä todetaan, että evästeiden tai muiden palvelun käyttöä kuvaavien tietojen tallentaminen ja käyttö on sallittua ainoastaan, jos palvelun tarjoaja antaa käyttäjälle ymmärrettävät ja kattavat tiedot tallentamisen ja käytön tarkoituksesta. Samalla käyttäjälle on annettava mahdollisuus kieltää evästeen tai muun tunnisteen tallentaminen päätelaitteelleen. Tiedonantovelvollisuutta ja käyttäjän kielto-oikeutta ei kuitenkaan tarvitse toteuttaa, jos 1) tietojen tallentamisen tai käytön ainoana tarkoituksena on toteuttaa viestin välittäminen viestintäverkoissa tai 2) tietojen tallentaminen tai käyttö on välttämätöntä sellaisen palvelun tarjoamiseksi, jota tilaaja tai palvelun käyttäjä on nimenomaisesti pyytänyt (esimerkiksi pankkipalvelu). Lisäksi säädetään, että tietojen tallentaminen ja käyttö on sallittua ainoastaan palvelun vaatimassa laajuudessa, eikä yksityisyyden suojaa saa rajoittaa enempää kuin on välttämätöntä. Tietojen ja kieltomahdollisuuden antaminen tulisi toteuttaa mahdollisimman käyttäjäystävällisellä tavalla. Annettavien tietojen on oltava myös selkeät ja kattavat, jotta käyttäjä osaa arvioida kielto-oikeuden käytön tarpeen. Palvelun tarjoajan ei kuiten-

kaan tarvitse koota kielto-oikeuden käyttäneistä rekisteriä, sillä kielto-oikeus koskee ainoastaan yksittäistä palvelun käyttökertaa. [HE 125/2003]

Selainohjelman asetuksia on toki mahdollista muuttaa pysyvästi siten, ettei selain hyväksy evästeitä ollenkaan tai kysyy jokaisesta evästeestä erikseen, hyväksyykö käyttäjä sen vai ei. Käytännössä vaihtoehto jäänee käyttämättä, sillä osatakseen määritellä itselleen sopivia asetuksia evästeteknologiasta tulisi ymmärtää edes perusasiat. Myös evästeiden poistaminen koneen muistista vaatii joko erillisen ohjelman tai asiantuntemusta ja omatoimisuutta. Lisäksi evästeitä käyttävä Internet-palvelu asettaa uuden evästeen poistetun tilalle, mikäli käyttäjä vierailee sivuilla uudelleen. Suurin käytännön ongelma on kuitenkin sivustojen toteutustekniikassa. Käytännössä käyttäjä pakotetaan hyväksymään evästeet, sillä ilman niitä sivustolle pääsy voi olla rajoitettua tai palvelu toimii epäluotettavasti.

Jo ennen sähköisen viestinnän tietosuojalain voimaanastumista tietosuojaviranomaiset ovat pitäneet käyttäjän tietämättä asetettavia evästeitä yksityisyyttä loukkaavana toimintana. Heinonen [2001b] arvostelee evästeitä erityisesti viranomaisomaistoiminnassa, sillä ne mahdollistavat kansalaisten tehokkaan valvonnan. Kaupallisten tahojen lisäksi myös jokin poliittinen tai ideologinen suuntaus voi asettaa evästeen käyttäjän koneeseen.

Nykyinen www-tekniikka ei enää pakota palvelujen kehittäjiä evästeiden käyttöön, sillä verkkosivustot ovat toteutettavissa muillakin keinoin. Esimerkiksi PHP-ohjelmointikieli mahdollistaa istuntokohtaisten muuttujien käytön, joissa käyttäjän antamat tiedot pysyvät tallessa palvelun käytön ajan. Istunnon aikana tarvittavat tiedot säilytetään palvelimelle tallennetussa tiedostossa, mikäli käyttäjä kieltää evästeet. Kun käyttäjä liikkuu palvelun sivulta toiselle, kulkee istuntokohtainen tiedoston identifioiva id-numero esimerkiksi piilotettujen lomakekenttien mukana. [Sessions; Session handling...] Sivuston eri käyttökertojen välillä tiedot voidaan puolestaan säilyttää tietokannassa, josta ne haetaan, kun asiakas on kirjautunut palveluun omalla käyttäjätunnus- ja salasanaparillaan.

6.3. Jälkien väärinkäyttö

Sinänsä harmittomia evästeitä on mahdollista käyttää väärin. Useimmiten väärinkäytökset liittyvät www-sivuille mainoksia myyviin palveluihin. Mainokset voidaan upottaa www-palvelun osaksi, jolloin ne tulevat eri palvelimelta kuin sivuston varsinainen sisältö, mutta käyttäjä ei tätä huomaa. Kun upotettujen mainosten mukana lähetetään kolmannen osapuolen evästeitä (*third-party cookie*), pystyy mainospalvelu seuraamaan, millä sivustoilla käyttäjä liikkuu. [Järvinen, 2002]

Pelkkä käyttäjien seuranta ei vielä mainostajia hyödytä, joten yritykset muodostavat on-line-kumppanuuksia, jotta henkilö saadaan myös tunnistettua. Tunnistus tapahtuu, kun jokin varsinaisen sisällön tarjoavista palveluista edellyttää käyttäjältä rekisteröintiä ja henkilötietojen luovuttamista. Mikäli sisältöpalvelu kuuluu mainostajan perustamaan yhteistyöverkostoon, ilmoittaa palvelu keräämänsä henkilötiedot myös mainostajalle.

Esimerkiksi www-mainostamisen kehittäjiin kuuluva DoubleClick käyttää asettamissaan evästeissä yksittäisen käyttäjän yksilöivää id-numeroa. Tunnisteen ja yhteistyöverkostonsa avulla DoubleClick kerää tietoja käyttäjien verkossa asioimisesta. Tietokantaan kerätyillä tiedoilla käyttäjälle kohdistetaan jatkossa tämän profiilia vastaavia mainoksia. Mainosten lähettämiseen liittyy myös seuranta siitä, mitä mainoksia käyttäjä valitsee tarkasteltavakseen. Yhteistyöverkostoon kuuluu tuhansia sivustoja, ja tiedot saattavat levitä mainostajan lisäksi minne tahansa muuallekin käyttäjän tietämättä. [Heinonen, 2001b; Järvinen, 2002] Myös hakupalvelut saattavat kerätä käyttäjätietoja. Esimerkiksi Google-hakupalvelu seuraa sen kautta tehtyjä hakuja IP-osoitteen ja käyttäjän työasemaan asetetun evästeen yhdistelmällä. Google saikin vuoden 2003 Iso Veli -palkinnon, sillä se rekisteröi käyttäjistään kaiken kerättävissä olevan tiedon eikä kerro, miksi tietoja kerää ja mihin tarkoitukseen. [Heinonen, 2003]

Evästeet voidaan myös yhdistää sähköpostiosoitteeseen, jos käyttäjä avaa HTML-koodatun sähköpostiviestin, johon eväste on upotettu. Kun viestissä oleva eväste aktivoituu, se tallentuu koneen muistiin samalla tavoin kuin www-sivultakin. Mikäli sähköpostiviestissä on www-linkki, jota vastaanottaja napsauttaa, eväste palautuu palvelimelle, ja viestin lukija on tunnistettu. [Järvinen, 2002]

Koska evästeiden käyttö on estettävissä, seurantaan on kehitetty myös verkkojäljitteitä (*web beacon*). Ne ovat linkkejä joko läpinäkyviin tai yhden kuvapisteen kokoisiin kuvatiedostoihin (*pixel beacon, web bug*), joita voidaan pienen kokonsa vuoksi upottaa huomaamattomasti www-sivulle tai sähköpostiviestiin. Kun kuva haetaan palvelimelta ja näytetään www-sivulla, se tuottaa merkinnän jäljittäjän lokiin ja kertoo, mistä osoitteesta sivu on avattu. Jäljitteiden ei tarvitse sijaita samassa palvelussa sivun varsinaisen sisällön kanssa, sillä kuvat voidaan linkittää mukaan mistä palvelinosoitteesta tahansa. Esimerkiksi Järvinen [2002] on löytänyt MTV 3:n pääsivulta kolme piilojäljitettä, joista yhden koodi on

```
<!-- Alma Media -->
<img src="http://stat.almamedia.fi/mtv3_c/t.gif" width="1"
height="1">.
```

Sähköpostiviestiin sijoitetun piilojäljitteen koodiin voidaan piilottaa vastaanottajan sähköpostiosoite, jolloin sekin tallentuu verkkojäljitteen lokiin. Juuri tästä syystä esimerkiksi roskapostit kannattaa tuhota suoraan niitä avaamatta, sillä viestin avaaminen vahvistaa roskapostittajalle osoitteen voimassaolon. Roskapostin lisäksi jäljitteitä käytetään erityisesti uutiskirjeissä, jolloin viestin lukemista voidaan seurata reaaliajassa rivi riviltä. [Järvinen, 2002]

HTML-koodatut viestit kannattaa lukea ilman verkkoyhteyttä (*offline*), jolloin jäljitteet eivät toimi. Lisäksi Privacy Foundation on julkaissut ilmaisen Bugnosis-ohjelman[7],

[7] http://www.bugnosis.org

joka analysoi www-sivut ja listaa tiedot niillä olevista jäljitteistä. Listauksen lisäksi ohjelma näyttää kuvasymboleina myös jäljitteiden sijainnin www-sivulla. [Järvinen, 2002]

Käyttäjiä seurataan myös vakoiluohjelmiksi (*spyware*) kutsutuilla sovelluksilla. Ohjelmat tulevat yleensä työasemaan huomaamattomasti jonkin toisen ohjelman mukana ja asentavat itsensä www-selaimen osaksi. Vakoiluohjelmilla saattaa olla myös jokin näennäinen tarkoitus, jonka varjolla niitä käyttäjille tarjotaan — esimerkiksi Gator mainostaa: "Less typing, faster shopping." Ohjelmien todellisena päämääränä on kuitenkin käyttäjän toimien seuraaminen ja mainosten näyttäminen. Selaimeen upotettuna seuraaminen onkin tehokkaampaa kuin evästeiden ja jäljitteiden kaltaisilla välillisillä tekniikoilla. [Järvinen, 2002]

Ohjelmat eivät välttämättä ole laittomia, sillä niiden tarkoitus kuvaillaan sovellusten kotisivuilla. Esimerkiksi VX2-ohjelmaa voidaan silti pitää vähintään kyseenalaisena, sillä se kerää jopa käyttäjän nimi- ja osoitetietoja täytetyiltä www-lomakkeilta. Vakoilusovelluksista on myös vaikea päästä eroon, sillä ne voivat selaimen lisäksi tallentua osaksi käyttöjärjestelmää. Mikäli vakoiluohjelman käynnistyskomento kopioituu järjestelmärekisteristä, edes käyttöjärjestelmän tai selaimen uudelleenasennus ei poista vakoilijaa. Lavasoft Ad-aware[8] on esimerkki paljastusohjelmasta, joka tunnistaa vakoilupalvelut ja osaa poistaa ne koneen rekisteristä. Paljastussovellusta on virustentorjuntaohjelmien tapaan syytä päivittää säännöllisesti, jotta se tunnistaisi uusimmatkin vakoilijat. [Järvinen, 2002]

6.4. Jälkien peittäminen

Internet-sivuilla voi toimia myös anonyymisti, mutta tällöin sähköisten jälkien peittämiseen on käytettävä erityisiä salauspalveluita. Yksinkertaisin tapa on liikennöidä salauspalvelun IP-osoitteen kautta, jolloin palvelu välittää sivujen hakupyynnöt ja palauttaa niihin tulevat vastaukset. Kehittyneempi salauspalvelu muun muassa väärentää käytetyn selaimen tiedot ja sotkee sen sivuhistorian. Käyttäjän valinnan mukaisesti palvelu joko poistaa evästeet tai muuttaa pysyvät evästeet istuntokohtaisiksi sekä salaa istunnon SSL-protokollalla (*secure sockets layer*). Tällaisia palveluja ovat esimerkiksi Anonymizer, Megaproxy ja Freedom Websecure. Kaikista kehittynein salauspalvelu vaatii tunnelointiohjelman asentamisen. Kun yhteys avataan oman operaattorin koneeseen, liikenne kuljetetaan salattua tunnelia pitkin anonyymipalvelimelle ja vasta sen jälkeen eteenpäin. [Järvinen, 2002]

Salauspalvelun huonona puolena on sen aiheuttama yhteys- ja laitteistokuormitus. Ilmaiset palvelut ovat huomattavan hitaita ja maksetunkin palvelun kautta liikennöinti hidastuu merkittävästi. Palveluita käytetään myös laittomaan toimintaan, joten anonyymipalvelinkin voi luovuttaa lokitietonsa viranomaisille, mikäli kyseessä on rikoksen epäily. [Järvinen, 2002]

[8] http://www.lavasoft.de

7. Yksityisyyden tukeminen tietoverkoissa

Tietoverkkojen aikakaudella näyttää siltä, ettei lainsäädäntö yksin riitä turvaamaan yksityisyyttä digitaalisissa toimintaympäristöissä. Tätä varten tarvitaan myös yksityisyyttä tukevaa tekniikkaa ja työkaluja (*privacy enchancing technology/tools, PET*). Kanadan informaatio- ja yksityisyysvaltuutettu Ann Cavoukian on arvellut PET-menetelmien olevan ainoa todellinen keino yksityisyyden suojaamiseksi. [Mantere, 1998] Tekniikan lisäksi yksityisyyttä voidaan tukea myös asenteilla — esimerkiksi yritys voi liittää tietosuojakäytänteet osaksi liiketoimintaprosessejaan.

7.1. Tietosuojapolitiikka

EU-maista poiketen Yhdysvalloissa luotetaan markkinoiden itsesäätelymekanismiin, jossa rekisterinpitäjiä eivät velvoita lait vaan liiketoiminnan realiteetit. Amerikkalaisessa liiketoimintamallissa lähdetään asiakastyytyväisyydestä, joten valtaosa yrityksistä kertoo itse vapaaehtoisesti, millä tavalla ne ovat ottaneet tietosuoja-asiat huomioon. Aarnio [2001b] kysyykin, onko lakiosasto edes oikea taho hoitamaan yrityksen tietosuoja-asioita, jotka saattaisivat sopia paremmin asiakaspalvelun vastattaviksi.

Yrityksen julkaisemasta tietosuojapolitiikasta (*privacy policy*) käyttäjille selviää, miten heidän henkilötietojaan käsitellään ja miten he voivat käyttää oikeuksiaan [Aarnio, 2001b]. Yritys puolestaan sitoutuu vapaaehtoisesti noudattamaan määrittelemiään tietojen keräämisen ja käytön periaatteita [Virtanen, 2002]. Tietosuojavaltuutettu Reijo Aarnio toivoo, että suomalaisetkin organisaatiot ymmärtäisivät tietosuojapolitiikan osaksi rekisterinpitäjän ja rekisteröidyn luottamussuhdetta [Toivonen, 2000].

Toisinaan tietosuojapolitiikka on kuitenkin nimellistä luottamuksellisuuden vakuuttelua, sillä sen sisältö saattaa tarkoituksellisesti olla juristin laatima ja maallikolle vaikeaselkoinen. Politiikkaan tutustumista voidaan myös hankaloittaa tekstin uuvuttavalla pituudella ja epämiellyttävällä käyttöliittymällä. Esimerkiksi Hotmail-sähköpostiohjelman 1058 riviä pitkä käyttösopimus tulisi lukea vieritettävästä tekstikentästä, josta tekstiä on kerralla näkyvissä kuuden rivin verran. Organisaatio saattaa myös muuttaa tietosuojapolitiikkaansa ja ilmoittaa asiasta vain kotisivullaan, eikä tieto muutoksista koskaan tavoita kaikkia käyttäjiä. [Järvinen, 2002]

Tietosuojapolitiikka voi olla muullakin tavoin epäluotettava. Vaikka evästeet kuvattaisiin hyvinkin tarkasti, jätetään piilojäljitteet useimmiten mainitsematta. Selkeiden väärinkäytösten ilmitullessa tietosuojan noudattamiseen sitoutunut organisaatio voi aina vedota virheeseen. Lisäksi pelkät periaatteet eivät auta hakkerin varastaessa henkilö- ja yhteystietoja huonosti suojatusta palvelusta. Taloudelliseen ahdinkoon joutuessaan yritykselle saattaa tulla ylitsepääsemätön houkutus myydä asiakkaittensa tietoja mainostajille. Konkurssin tehneen yrityksen tiedot ehkä päätyvät uuteen käyttöön ilman vanhojen sopimuksien velvoituksia. [Järvinen, 2002]

7.2. P3P-standardi

Anonyymipalveluiden lisäksi yksityisyyttä voidaan varjella verkkopalveluissa muillakin tekniikoilla. W3-konsortion P3P-projekti (*platform for privacy prefenrences*) on kehittänyt standardoidun tavan www-palvelun tietosuojapolitiikan ilmaisemiseen. Tavoitteena on, että käyttäjä saa informaation organisaation julkaisemasta tietosuojapolitiikasta yksinkertaistetussa ja ymmärrettävässä muodossa ilman monimuotoisten tekstien uuvuttavaa läpikäymistä. Kun organisaatio ilmaisee tietosuojapolitiikkansa standardilla tavalla, voi selain (*user agent*) tulkita politiikan nopeasti ja automaattisesti käyttäjän ymmärtämään muotoon. Standardi ei kuitenkaan takaa sitä, että yritykset todella myös noudattavat julkaisemaansa tietosuojapolitiikkaa. [Platform for Privacy..., 2002; P3P and Privacy..., 2002]

Ideana on, että selain ilmoittaa käyttäjälle, mikäli palvelun P3P:llä kuvattu tietosuojapolitiikka ei vastaa selaimeen tehtyjä valintoja. Esimerkkinä olkoon vaikkapa käyttäjän asettama vaatimus SSL- tai SET-tietoturvaprotokollasta (*Secure Electronic Transactions*), mikäli sivusto vaatii rekisteröityvän luottotietoja. Jos verkkopalvelu ei täytä annettua ehtoa, hälyttää selain ja osoittaa käyttäjälle, miten politiikka poikkeaa tämän mieltymyksistä. P3P:n avulla käyttäjän on mahdollista myös valita, millaisia evästeitä hän hyväksyy. Aiemminhan evästeiden automatisoitu erottelu ei ollut mahdollista, eikä niiden käyttötarkoituksesta saanut riittävästi tietoa. Lisäksi P3P mahdollistaa erilaisten tietosuojapolitiikkojen käytön verkkopalvelun kullekin eri osioille tai toiminnolle. Esimerkiksi etusivulla voidaan kerätä pelkästään HTTP-standardiin kuuluvaa verkkoliikennöintitietoa, mutta ostoskorin käyttö vaatii jo henkilökohtaisemman tiedon luovuttamista. [Platform for Privacy..., 2002; P3P and Privacy..., 2002]

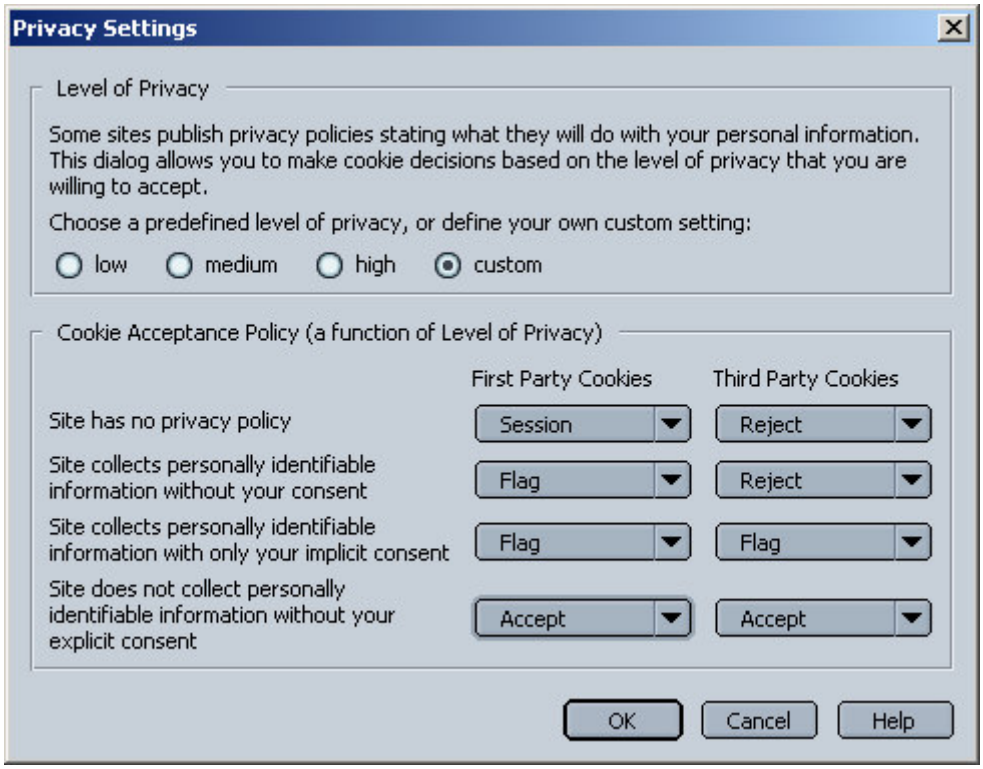
P3P:n kehitystyö on ollut pitkä prosessi. Standardin tarkoituksena oli alunperin mahdollistaa myös automatisoidut tiedonsiirrot sekä käyttäjän ja palveluntarjoajan välinen neuvottelu. Ominaisuudet jäivät pois osaksi sen vuoksi, että P3P:n ensimmäinen versio haluttiin vihdoin saada käyttöön, ja lisäominaisuuksien kehittely olisi viivyttänyt entisestään hidasta kehitystyötä. Toisena merkittävänä syynä oli tietosuojaviranomaisten vastustus automaattista tietojen siirtoa kohtaan. Viranomaiset pelkäsivät, että standardoidun tiedonsiirron avulla henkilötietojen keruu tulee yrityksille yhä vain helpommaksi. P3P:n kehitystyötä jatketaan, ja tulevissa versiossa tiedonsiirto saattaa olla mahdollista. Standardin kehittäjienkin nykyinen kanta on, ettei selaimien oletusarvoksi tule asentaa käyttäjän tietämättä tapahtuvaa, automaattista henkilötietojen siirtoa. [Platform for Privacy..., 2002; P3P and Privacy..., 2002]

EU:ssa on suhtauduttu P3P-standardiin kriittisesti protokollan matalan standarditason ja teknisen painotuksen vuoksi. P3P:n kehitys on aloitettu Yhdysvalloissa, jossa yksityisyyttä koskevat standardit ovat alhaisemmalla tasolla kuin tiukkaan sääntelyyn tottuneessa EU:ssa. [Mantere, 1998; Heinonen, 1998b] Informaatio- ja yksityisyysvaltuutettu Cavoukian on kuitenkin todennut, että jostakin täytyy vain aloittaa. Vaikka teknisten termien mieltäminen sosiaalisten toimintojen osaksi on hankalaa, P3P-protokollassa

on sentään ryhdytty luomaan yhteisesti hyväksyttävää kieltä henkilötietojen käyttöön verkkopalveluissa [Mantere, 1998]. W3C:n sivulla[9] on laaja kokoelma linkkejä P3P:tä kritisoiviin tai muuten kommentoiviin kirjoituksiin.

Standardin kehittäjien kanta on, ettei P3P:tä ole tarkoitettukaan ratkaisemaan yksinään verkkopalveluihin liittyviä tietosuojaongelmia. Sen sijaan standardi täydentää sekä itsesäätelyyn että lainsäädäntöön nojaavia käytäntöjä. P3P:stä on hyötyä esimerkiksi palveluntarjoajalle asetetun informointivelvoitteen täyttämisessä. Standardin teknispainotteisuuden avuksi oletetaan kehitettävän työkaluja. Voihan HTML-kieltä ymmärtämätönkin melko helposti luoda www-sivuja tähän tarkoitukseen tehdyillä editoreilla ilman yksityiskohtaista HTML-koodin tuntemusta. [P3P and Privacy..., 2002]

Sekä Internet Explorer 6.0 että Netscape 7.0 -selaimissa on mahdollista eritellä kolmannen osapuolen ja varsinaisen palveluntarjoajan asettamien evästeiden käsittely (Kuva 9). Selainasetukset voi esimerkiksi määritellä sallimaan ainoastaan palvelun lähettämät istuntokohtaiset evästeet. Kummassakin selainohjelmassa on mahdollista tallentaa jopa pysyviä, yksittäisiä sivustoja koskevia määrittelyjä (*per site privacy actions, managing cookies site-by-site*).



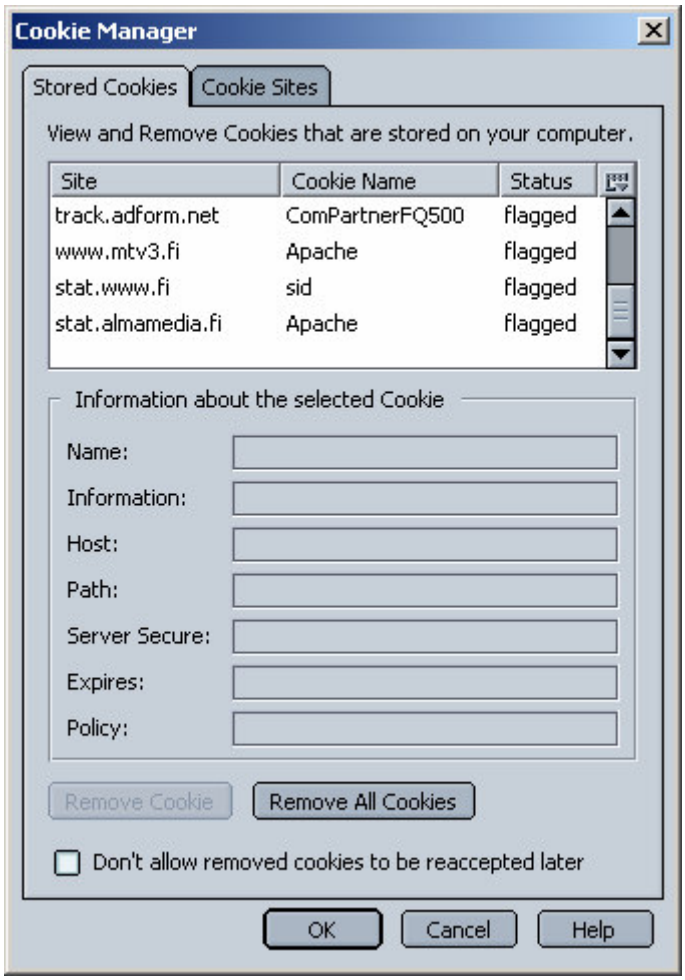
Kuva 9. Netscape 7.0 -selaimen asetusvaihtoehtoja evästeiden käsittelyyn.

Käyttäjän tekemistä valinnoista poikenneesta evästeestä ilmoitetaan ohjelman tilarivin (*status bar*) oikeassa reunassa näkyvällä ikonilla. Internet Explorer näyttää lisäksi ikkunan, jossa ikonin olemassaolosta tiedotetaan (Kuva 10). Ilmoitus onkin tarpeen, sil-

[9] http://www.w3.org/P3P/

lä ikoni on melko huomaamaton, eikä sen ilmestymistä tilariville havaitse, ellei tilannetta osaa erityisesti tarkkailla. Ikonia napsauttamalla kummassakin selaimessa on mahdollista tarkastella raporttia, joka sisältää tarkemmat tiedot sivuston asettamista evästeistä (Kuva 11).

Kuva 10. Internet Explorer 6.0:n käyttämä ilmoitus.



Kuva 11. Netscape 7.0:n evästeistä tilastoimia tietoja.

Yksityisyyden suojaa koskevia selainasetuksia on jaettu moneen dialogiin, joten niiden hallinta on kohtalaisen monimutkaista ja vaatii aiheeseen perehtymistä. Ohjelmien on-line-manuaaleista löytyy toki aihetta käsittelevää ohjeistusta, mutta esimerkiksi Netscapen *Using Privacy Features* -ohje on paperille tulostettuna 18 sivua pitkä.

7.3. Asenteet ja tietoisuus tietosuojasta

Kansalaisten tietämys tietosuoja-asioista on melko alhainen eikä yksityisyyden oikeutta tunneta hyvin. Vuonna 1996 EU-komission teettämän Eurobarometer-tutkimuksen mukaan alle 30 % suomalaista yleensäkin tiesi heillä olevan yksityisyyden suojan oikeuksia, kun esimerkiksi Hollannissa vastaava luku oli 60 % [Kuopus, 1997b]. Vuonna 2004 tietosuojavaltuutettu huomautti, ettei kansalaisten tietoisuus omista oikeuksistaan rekisteröityinä ole vieläkään riittävä [Aarnio, 2004]. Paradoksaalisesti tietosuoja-asioitten tiedottamis- ja neuvontavelvollisuus on nimenomaan tietosuojaviranomaisilla. Tietosuojaviranomaiset ovat omasta puolestaan tiedostaneet tämän haasteen, ja Aarnio [2004] kertoo tietosuojavaltuutetun toimiston ottaneen käyttöön uuden tiedotussuunnitelman ja uudistavan myös verkkosivujaan. Myös hallituksen vuonna 2003 hyväksymässä tietoyhteiskuntaohjelmassa on todettu, että tietosuojavaltuutetun toimiston lisäresursointi muun muassa viestinnän tehostamiseksi on yksi tietoyhteiskuntakehitystä edistävistä toimenpiteistä [Harjuhahto-Madetoja, 2004].

Tietosuojan huonosta tuntemuksesta ei voi moittia pelkästään suomalaisia. Myös Euroopan unionin puiteohjelmien siirtymävaiheessa tehdyssä tilannearviossa on vuonna 2003 todettu, että yksityisyyden suojasta vallitsee huomattava tietämättömyys. Samalla EU-komissio esittää, että

— on kehitettävä uusia on-line-tietosuojamalleja
— liiketoimintamallit on uudistettava tietosuojan avulla ja tietosuoja on otettava liiketoimintaprosessien osaksi
— tietosuoja on liitettävä systeemisuunnitteluun
— koulutusta on lisättävä
— on luotava tietosuojaa tukevaa IT-infrastruktuuria ja
— tietosuojaloukkaukset on estettävä teknologian avulla.

Myös lainsäädäntöön suunniteltaneen muutoksia. [Aarnio, 2004]

Suomessa tietosuojaviranomaiset ovat pohtineet muun muassa tietojärjestelmien suunnittelutyöhön liitettävää vaatimusta henkilötietojen käsittelyä koskevasta etukäteissuunnittelusta. Lisäksi seurantajärjestelmän kehittäminen rangaistus- ja seuraamusjärjestelmien toimivuudesta saattaisi olla aiheellista. Organisaatioihin olisi mahdollista nimetä tietosuojavastaavia ja kuntiin tietosuoja-asiamiehiä. Tietosuoja-asioiden osaamisen lisäämiseksi tietosuoja voitaisiin sisällyttää opetusohjelmiin. [Kleemola, 2003] Lisäksi tarvittaisiin koordinoitua teknologian vaikutusten arviointia tekevä taho — esimerkiksi Ruotsissa sitä varten on perustettu kansallinen elin [Aarnio, 2001a]. Tietosuojan toteuttamista ei kuitenkaan voi sälyttää pelkästään yritysten ja julkisen hallinnon harteille.

Nurmi [2002] painottaakin, että myös kansalaisilta edellytetään valppautta tietojen käytössä sekä omista oikeuksistaan huolehtimista.

Tilastokeskus on tutkinut suomalaisten käsityksiä tietojensa rekisteröinnistä vuosina 1997 ja 2000. Vuonna 2000 vastanneista 77 % oli sitä mieltä, ettei pankki- ja luottokorttien käyttöä tarvinnut välttää verkkosovelluksissa yksityisyyden suojan vaarantumisen vuoksi. Lisäksi yli puolet vastaajista piti esimerkiksi kanta-asiakaskorteilla saatavia etuja tärkeämpinä kuin niihin liittyviä yksityisyyden suojan uhkia. Muutenkaan tutkimuksessa ei ilmennyt erityistä huolta tietojen rekisteröinnistä ja käytöstä. Tästä huolimatta 69 % kaikista vastanneista halusi tietää, mitä tietoja heistä kerätään tietoverkossa asioimisen yhteydessä. Internetiä paljon käyttävistä 78 % halusi tietää tietojensa keräämisestä. [Heinonen, 2000]

Yritysmaailman osalta tietosuojavaltuutettu Reijo Aarnio [2001b] toteaa, että yrityksiä vaivaa tietosuoja-asioiden toteuttamisessa pikemminkin tahdon kuin taidon puute. Sen sijaan, että tietosuojasta huolehtiminen olisi osa hyvin hoidettua asiakaspalvelua, vallitsevaa asennetta voi kuvata vastahakoinen tokaisu: "Pitääkö meidän todellakin informoida asiakkaitamme?" Tietosuojavaltuutetun toimistoon saapuvista valituksista päätellen erityisesti IT-ala vaikuttaa lähinnä villiltä länneltä tietosuojalakien huomioimisen suhteen. Aarnio [2001a] on huolissaan oma-aloitteisen itsekritiikin puutteesta ja muistuttaa yrityksiä siitä, ettei teknologia sellaisenaan tuo oikeuksia. Tietosuojavaltuutettu ehdottaakin virtuaalipoliisin perustamista Suomeen selvittämään ja valvomaan tietosuojarikoksia Internetissä. Virtuaalipoliisia tarvittaisiin, sillä tietosuojavaltuutetun toimistolla ei ole resursseja ja teknistä osaamista uuden teknologian mukanaan tuomien ongelmien ratkomiseen. [Toivonen, 2000]

Internetiä leimaavat muun muassa huijaukset, joten luottamuksen rakentaminen on tietoverkossa pitkäjänteistä toimintaa. Siksi yksityisyyden suojasta huolehtiminen kannattaisi sisäistää osaksi yrityksen strategiaa ja toimintatapoja. Mainetta rakentavan organisaation on muutettava toimintatapojaan pysyvästi. Tietosuoja tulisi nähdä tietojärjestelmähankkeiden luonnollisena osana jo projektin tarjouspyyntö- ja määrittelyvaiheesta alkaen. Mikäli tietosuoja irrotetaan muusta toiminnasta, tulee siitä helposti erillinen projekti, joka toteutetaan jos keritään. Kustannuksia kurissa pidettäessä tietosuoja on usein ensimmäisten poispudotettavien asioiden joukossa. Toisinaan tietosuoja-asioitten toteuttamatta jättämistä saatetaan perustella jopa käyttäjäystävällisyyden nimissä. [Aarnio, 2000; Virtanen, 2002]

Luotettava yritys kerää tietoja avoimesti ja käyttää niitä kansalaisten hyväksymällä tavalla. Luotettavaksi profiloituva organisaatio saa myös kilpailuetua. Hyvän maineen saavuttaneen yrityksen arvostus kasvaa ja samalla hinnoittelun vapaus lisääntyy. Kun hinnalla ei tarvitse enää kilpailla, syntyy brandi. Silti myös kohderyhmä on tunnettava: osa asiakkaista arvostaa luotettavuutta, toiset tinkivät vaatimuksista halvan hinnan tai muiden etujen takia. Kumpikin ryhmä tarvitsee toimittajansa, mutta yrityksen tulee tietoisesti valita, kummalle se tuotteitaan tarjoaa. [Virtanen, 2002]

Julkisella sektorilla on omat erityishankaluutensa, sillä sen toimintaa koskevia säännöksiä löytyy niin tietoturvallisuussäännöksistä kuin julkisuus-, salassapito-, arkisto- ja tietosuojalainsäädännöstäkin. Avuksi voidaan kuitenkin ottaa hyvä tiedonhallintatapa, joka ohjaa viranomaisia säännösten viidakossa esimerkiksi tietojärjestelmiä uudistettaessa. Hyvän tiedonhallintatavan ohjeita noudattaen säännöksiä pystytään soveltamaan samanaikaisesti ja johdonmukaisena kokonaisuutena. Hyvässä tiedonhallintatavassa huolehditaan erityisesti tietojen laatuun vaikuttavista tekijöistä, kuten saatavuudesta, eheydestä, käytettävyydestä ja suojaamisesta. Apuna voidaan käyttää myös arkistonmuodostamissuunnitelmaa, jonka sivutuotteena syntyy myös henkilötietolain vaatima rekisteriseloste. [Wallin, 1998]

7.4. Mahdollisia valvonnan kehityssuuntia

Yrityksen itse itselleen laatima tietosuojapolitiikka ei ilmeisestikään sido yritystä juridisesti. Tietosuojapolitiikan laatimisella on kuitenkin merkitystä, sillä se pakottaa Internet-palvelujen tarjoajat miettimään käytänteitään. Sen vuoksi saattaisi olla perusteltua vaatia, että jokainen henkilötietoja käsittelevä verkkopalvelu julkaisisi sivuillaan tietosuojapolitiikan selaimen ymmärtämässä XML-formaatissa (*eXtensible Markup Language*). Mikäli politiikka puuttuisi sivustolta, voisi selain hälyttää käyttäjää ja lähettää asiasta ilmoituksen tietosuojaviranomaisille. Täten sivustojen valvontaa voitaisiin samalla kehittää automatisoituun suuntaan.

Verkkopalvelujen tarkistusta kannattaisi muullakin tavoin mahdollisuuksien mukaan automatisoida. Palveluntarjoajille voitaisiin laatia esimerkkiformaatti, jota henkilötietoja käsittelevällä sivustolla tulisi henkilötietojen käsittelyn kohdalla noudattaa. Formaalia kuvauskieltä noudattavalta sivustolta rekisteriselosteen, käyttäjien informoinnin ja vastaavien seikkojen toteutus olisi teknisesti tarkistettavissa. Lisäksi tietosuojavaltuutetun toimisto tai muu vastaava viranomaistaho voisi laatia rekisterinpitäjille valmiita XML-kuvauskielellä tehtyjä toteutusmalleja.

Evästeiden, piilojäljitteiden ja muiden tunnisteiden laittoman käytön estämiseksi sivuston koodin tulisi olla tarkistettavissa. Koodi ei välttämättä voi olla täysin julkista, sillä se saattaisi paljastaa järjestelmätoteutuksesta tietoja, joita ei ole tietoturvasyistä tarpeen tuoda ulkopuolisten tietoon. Siksi koodin voisikin tarkistaa jokin luotettava kolmas osapuoli, joka antaisi palveluntarjoajalle todistuksen laillisesta toteutustavasta. Mikäli todistus puuttuisi tai olisi vanhentunut, voisi selain edelleen tehdä asiasta hälytyksen sekä käyttäjälle että valvovalle viranomaiselle.

8. Yhteenveto

Tietoyhteiskuntaohjelman tavoitteena on tietoyhteiskuntapalveluiden ulottaminen kaikkien saataville. Samaan aikaan henkilötietojen käyttömahdollisuudet kaupallisiin ja valvonnallisiin tarkoituksiin kasvavat. Mitä suurempi osa henkilötiedoista liikkuu tietoverkoissa, sitä paremmat mahdollisuudet eri tahoilla on näiden tietojen hyödyntämiseen. Henkilötietolaissa esitellään selkeät ohjausperiaatteet, joita noudattamalla rekisterinpitäjä voi toimialastaan riippumatta järjestää henkilötietojen käsittelyn siten, että rekisteröityjen oikeusturva säilyy. Suomessa on myös hyvin järjestetty viranomaistoiminta, joka takaa sen, että rekisterinpitäjä saa tietosuoja-asioiden pulmatilanteissa apua ongelmiinsa. Näistä seikoista huolimatta sekä yksityiset että julkiset Internet-palvelujen tarjoajat jättävät, jopa tietoisesti, lainsäännösten asettamat velvoitteet huomiotta. Harva rekisterinpitäjä informoi rekisteröimiään henkilöitä heidän tietojensa käsittelystä. Rekisteröidyillä ei yleensä ole mahdollisuutta kieltää itseensä kohdistuvaa suoramarkkinointia — tai mikäli mahdollisuus on, se on hankalasti toteutettavissa. Lisäksi henkilötietoja tulisi kerätä ainoastaan perustellusti ja ennalta määriteltyyn tarpeeseen sitä unohtamatta, että rekisterinpitäjällä ja rekisteröitävällä tulisi olla asiallinen yhteys, jotta yrityksellä ylipäätään on oikeus henkilötietojen käsittelyyn.

Tällä hetkellä tietosuojalainsäädännön selkein ongelma on lain noudattamisen valvonta. Rekisterinpitäjät käyttävät tilannetta hyväkseen eikä henkilötietolakiin kirjattu ajatus rekisterinpitäjän itseohjautuvuudesta tietosuojaperiaatteiden noudattamisessa selvästikään toteudu. Ongelmaa pahentaa se, etteivät rekisteröitävät henkilöt juurikaan tiedä tai välitä oikeuksistaan. Yleisöpaine vaikuttaa rekisterinpitäjiin, joten mikäli kansalaiset olisivat tarkempia omien henkilötietojensa käsittelystä, osa lainsäädännön valvontaongelmista tulisi samalla hoidetuksi. Tietosuojaviranomaisten tavoitteena onkin lisätä yleistä tietosuoja-asioiden tietämystä. Keinoina aiotaan käyttää muun muassa koulutusta ja tiedottamisen lisäämistä. Kansalaisten ei kuitenkaan voida olettaa yksinään ryhtymään tietosuojapoliiseiksi, joten myös lainsäädännön noudattamista pyritään tehostamaan. Tulevaisuudessa tähän tarkoitukseen saatetaan perustaa uusi valvontaan keskittyvä viranomaistaho. Toisaalta on käynyt selväksi, ettei pelkkä lainsäädäntö eikä edes tehostettu valvontamekanismi riitä takaamaan yksityisyyden suojan toteutumista. Niinpä avuksi on ryhdytty kehittämään myös yksityisyyttä tukevaa teknologiaa, joka tulevaisuudessa mahdollisuuksien mukaan jopa automatisoi tietosuoja-asioiden noudattamista.

Sekä kansallisen että Euroopan sisämarkkinoita säätelevän tietosuojalainsäädännön tarkoituksena on taata turvallinen ja luotettava tietoyhteiskunta. Siksi lainsäädännössä on vielä toistaiseksi pitäydytty linjalla, jossa yksityinen henkilö nähdään rekisterinpidon heikompana ja siten myös suojeltavana osapuolena. Esimerkiksi vastikään voimaantulleessa sähköisen viestinnän tietosuojalaissa vastuu sähköisistä jalanjäljistä asetetaan selvästi rekisterinpitäjälle. Samalla yksityisten henkilöiden kulutus- ja asiointitottumusten seurantaa on haluttu rajoittaa. On tietenkin mahdollista, ettei kansalaisten kiinnostus

omien henkilötietojensa käsittelyä kohtaan lisäänny mistään toimista huolimatta. Tällöin jää mietittäväksi, onko nyky-yhteiskunnan kehitys kulkemassa yhteisesti hyväksytyllä tavalla suuntaan, jossa oikeus anonymiteettiin on menetetty eikä julkista holhousta kaivata? Vai käykö yksityisyyden kanssa siten, että sen menettämisen merkitys ymmärretään vasta sitten, kun vallalle on peruuttamattomasti päässyt käytänteitä, jotka eivät jätä yksityisyyden suojalle sijaa? Tulevaisuudessa rekisterinpitäjien tiedollinen ylivalta yksityiseen henkilöön nähden saattaa kasvaa ennalta arvaamattomiin mittoihin. Järvinen [2002] toteaakin, etteivät kuluttajat vielä tiedä mikä kaikki on mahdollista — mutta toistaiseksi sitä eivät tiedä yrityksetkään.

Viiteluettelo

[Aarnio, 1999] Reijo Aarnio, Aito Asia. *Tietosuoja* **12**, 3 (1999), 3.

[Aarnio, 2001a] Reijo Aarnio, Vaikutuksia. *Tietosuoja* **14**, 3 (2001), 3.

[Aarnio, 2001b] Reijo Aarnio, Privacy Policy. *Tietosuoja* **14**, 4 (2001), 3.

[Aarnio, 2003] Reijo Aarnio, Mitä yksityisyyden suoja on. *Tietosuoja* **16**, 1 (2003), 10—13.

[Aarnio, 2004] Reijo Aarnio, Tietosuojavaltuutetun katsaus vuoteen 2003: Ennennäkemätön virusvuosi horjutti uskoa tietoverkkojen turvallisuuteen. *Tietosuoja* **17**, 2 (2004), 28—31.

[Ammattiyhdistyksen jäsenten..., 2003] Ammattiyhdistyksen jäsenten sähköpostiosoitteiden julkaiseminen Internet-verkossa. Henkilötietolain mukaisia kannanottoja. *Tietosuoja* **16**, 2 (2003), 34.

[2002/58/EY] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi). http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FI&numdoc=32002L0058&model=guichett (tarkastettu 30.9.2004).

[95/46/EY] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fi&numdoc=31995L0046&model=guichett (tarkastettu 13.9.2004).

[HaVM 26/1998] Hallintovaliokunnan mietintö 26/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Vuoden 1998 valtiopäivät. Asiakirjat C2 Valiokuntien mietinnöt ja lausunnot. Edita, Helsinki, 2000.

[HE 49/1986] Hallituksen esitys Eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi. Asiakirjat A1 Hallituksen esitykset 1—50. Vuoden 1986 valtiopäivät. Valtion painatuskeskus, Helsinki, 1986.

[HE 96/1998] Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Asiakirjat A3 Hallituksen esitykset 71—104. Vuoden 1998 valtiopäivät. Edita, Helsinki, 1998.

[HE 125/2003] Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi. Saatavana hakulauseella "125/2003" Finlex-säädöskokoelman osoitteesta http://www.finlex.fi/esitykset/index.html (tarkastettu 23.9.2004).

[Harjuhahto-Madetoja, 2004] Katrina Harjuhahto-Madetoja, Tietoyhteiskuntaohjelma osana hallitusohjelmaa. *Tietosuoja* **17**, 1 (2004), 4—6.

[Heinonen, 1994] Risto Heinonen, Tietosuoja on eettinen valinta. *Tietosuoja* **6**, 2 (1994), 17—20.

[Heinonen, 1996] Risto Heinonen, Onko tietotekniikka ajanut tietosuojalainsäädännön ohi? *Tietosuoja* **9**, 4 (1996), 11—17.

[Heinonen, 1997] Risto Heinonen, Tietosuojan uudet haasteet. *Tietosuoja* **10**, 3 (1997), 20—23.

[Heinonen, 1998a] Risto Heinonen, Tietovarastojen kaupallinen hyödyntäminen ja tietosuoja. *Tietosuoja* **11**, 1 (1998), 25—30.

[Heinonen, 1998b] Risto Heinonen, Globaali verkko vaatii globaaleja keinoja. *Tietosuoja* **11**, 3 (1998), 23—26.

[Heinonen, 2000] Risto Heinonen, Suomalaisten mielipiteet tietojensa rekisteröinnistä ja yksityisyydestä. *Tietosuoja* **13**, 2 (2000), 21—24.

[Heinonen, 2001a] Risto Heinonen, *Digitaalinen minä.* Edita, Helsinki, 2001.

[Heinonen, 2001b] Risto Heinonen, Yksityisyys pipariksi. *Tietosuoja* **14**, 1 (2001), 26—31.

[Heinonen, 2003] Risto Heinonen, Tapahtumatietojen käsittely — tietosuojan harmaa alue. *Tietosuoja* **16**, 4 (2003), 10—15.

[HenkRekL] Henkilörekisterilaki 30.4.1987/471.

[Henkilötietojen käsittelyä..., 1999] Henkilötietojen käsittelyä koskeva lainsäädäntö muuttui 1.6.1999 lukien. *Tietosuoja* **12**, 2 (1999), 8—14.

[HetiL] Henkilötietolaki 22.4.1999/523.

[Hyvään rekisteritapaan..., 1997] Hyvään rekisteritapaan kuuluu, että rekisteröidylle annetaan oikea ja selkeä kuva hänen oikeuksistaan. Tietosuojalautakunnan päätöksiä (27/97). *Tietosuoja* **11**, 1 (1998), 38—39.

[Järvinen, 2002] Petteri Järvinen, *Tietoturva & yksityisyys.* Docendo Finland, Porvoo, 2002.

[Kara, 2002] Eija Kara, Verkkopalvelut unohtavat käyttäjän informoinnin henkilötietoja kerättäessä. *Tietosuoja* **15**, 4 (2002), 36—38.

[Kleemola, 2003] Maija Kleemola, Katsaus tietosuojavaltuutetun toimiston 15 vuoteen. *Tietosuoja* **16**, 1 (2003), 4—9.

[Klemetti, 1998] Jari Klemetti, Tietosuoja ja henkilötietojen kaupallinen hyödyntäminen. *Tietosuoja* **11**, 4 (1998), 4—9.

[Konstari, 1992] Timo Konstari, *Henkilörekisterilaki. Säännökset ja käytäntö.* Gummerus, Jyväskylä, 1992.

[Konstari, 1997] Timo Konstari, Matkalla kohti eurooppalaista tietosuojaa. *Tietosuoja* **10**, 4 (1997), 18—22.

[Korpela, 2003a] Jukka Korpela, Yksilönsuoja ja sananvapaus riitasilla. *Datatekniikka ja viestintä*. http://www.cs.tut.fi/~jkorpela/hlorek.html (tarkastettu 18.6.2004).

[Korpela, 2003b] Jukka Korpela, Henkilörekistereistä lain kannalta. *Datatekniikka ja viestintä*. http://www.cs.tut.fi/~jkorpela/bb2003.html (tarkastettu 18.6.2004).

[Kuopus, 1995] Jorma Kuopus, Yksilön oikeuksista tietoverkoissa. *Tietosuoja* **8**, 1 (1995), 3.

[Kuopus, 1996] Jorma Kuopus, EU:n tietosuojadirektiivi ja henkilörekisterilain tarkistaminen. *Tietosuoja* **9**, 3 (1996), 21—25.

[Kuopus, 1997a] Jorma Kuopus, Tietosuojan uudet haasteet suoramarkkinoinnissa. *Tietosuoja* **10**, 1 (1997), 4—8.

[Kuopus, 1997b] Jorma Kuopus, Suomalaisten käsityksiä tietosuojastaan. *Tietosuoja* **10**, 3 (1997), 3.

[Käyttäjälokin tietojen..., 2003] Käyttäjälokin tietojen käsittely henkilötietolain mukaan. Asiaa tietosuojasta 1/2003 10.2.2003. Tietosuojavaltuutetun toimisto.

[Lausunto Väestörekisterikeskukselle..., 2004] Lausunto Väestörekisterikeskukselle 28.1.2004. Kuluttajavirasto. http://www.kuluttajavirasto.fi/user_nf/default.asp?id=14418&site=34&tmf=7418&root_id=7418&mode=readdoc (tarkastettu 2.9.2004).

[Mahkonen, 1997] Sami Mahkonen, *Oikeus yksityisyyteen.* WSOY, Porvoo, 1997.

[Mantere, 1998] Tiina Mantere, Web puhutti pyhiinvaeltajien keskellä. *Tietosuoja* **11**, 3 (1998), 18—22.

[MAO: 119/03] Markkinaoikeus. Dnro 173/02/M2. Antopäivä 10.6.2003. http://www.oikeus.fi/markkinaoikeus/20084.htm (tarkastettu 30.9.2004).

[Niku-Paavo, 2003] Sari Niku-Paavo, Mitä käytännesäännöt ovat? *Tietosuoja* **16**, 1 (2003), 18—21.

[Nurmi, 2002] Pekka Nurmi, Tietoisuus tietosuojasta. *Tietosuoja* **15**, 4 (2002), 8.

[Näkökohtia henkilötietojen..., 2002] Tietosuojavaltuutetun toimisto: Näkökohtia henkilötietojen käsittelystä asiakassuhteessa sekä asiakkaaseen kohdistuvasta suoramarkkinoinnista. *Tietosuoja* **15**, 3 (2002), 25—28.

[Opiskelijoiden kurssiarvostelujen..., 2001] Opiskelijoiden kurssiarvostelujen vieminen Internetiin. Henkilötietolain mukaisia kannanottoja. *Tietosuoja* **14**, 3 (2001), 28.

[Oppilaiden henkilötietojen..., 2002] Oppilaiden henkilötietojen vieminen koulun kotisivulle. Henkilötietolain mukaisia kannanottoja. *Tietosuoja* **15**, 2 (2002), 29.

[P3P and Privacy..., 2002] P3P and Privacy on the Web FAQ. W3C Platform for Privacy Prefenrences Initiative. http://www.w3.org/P3P/p3pfaq.html (tarkastettu 3.8. 2004).

[Partanen, 1995] Heikki Partanen, Tietosuojan kaksi puolta — yksityisyyden suoja ja erilaiset tietotarpeet yhteiskunnassa. *Tietosuoja* **8**, 1 (1995), 4—8.

[Partanen, 1996] Heikki Partanen, Direktiivi, tietosuoja ja sietämätön hämäryys. *Tietosuoja* **9**, 2 (1996), 11—14.

[Partanen, 2004] Heikki Partanen, Tietosuojavaltuutetun toimisto. Henkilökohtainen tiedonanto 23.9.2004.

[Platform for Privacy..., 2002] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Recommendation 16 April 2002. http://www.w3.org/TR/P3P/ (tarkastettu 3.8.2004).

[Puukka, 2001] Arja Puukka, Yhdistyksen jäsenrekisterit henkilörekistereinä. *Tietosuoja* **14**, 2 (2001), 28—29.

[Saarenpää, 1992] Ahti Saarenpää, Oikeusinformatiikka: tiedettä ja toimintaa. Teoksessa Antti Rautava ja Kaisa Sinikara (toim.) *Tietohuolto ja juridiikka.* 1992, 101—117.

[Saarenpää, 1994] Ahti Saarenpää, Tieto ja suoja. Teoksessa Ilkka Saraviita et al. (toim.) *Juhlajulkaisu oikeustieteen ylioppilaiden yhdistys Artikla ry 15 vuotta.* Oikeustieteen ylioppilaiden yhdistys Artikla ry, 1994, 153—186.

[Saarenpää, 2004] Ahti Saarenpää, Yksityisyyden suoja tietämättömyyden yhteiskunnan uteliaisuusympäristössä. *Tietosuoja* **17**, 1 (2004), 12—19.

[Sessions] Sessions. http://www.free2code.net/plugins/articles/read.php?id=184 (tarkastettu 30.9.2004).

[Session handling...] XCVI. Session handling functions. Passing the Session ID. PHP Manual. http://fi2.php.net/manual/en/print/ref.session.php (tarkastettu 30.9.2004).

[PeL] Suomen perustuslaki 11.6.1999/731.

[SVTSL] Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

[Tietojen rekisteröinti..., 1997] Tietojen rekisteröinti verkkolehden lukemisen yhteydessä. Tietosuojavaltuutetun kannanottoja. *Tietosuoja* **10**, 3 (1997), 25.

[KM 1981/66] Tietosuojakomitean mietintö. Komitean mietintö 1981:66. Valtion painatuskeskus, Helsinki.

[Toivonen, 2000] Sarianna Toivonen, Tietosuojavaltuutettu toivoo virtuaalipoliisia. Suomen Tietotoimiston uutisia. *Tietosuoja* **13**, 4 (2000), 37.

[Uudet sähköisen..., 2002] Uudet sähköisen kuluttajakaupan käytännesäännöt sallivat lupapyyntöspämmin. Electronic Frontier Finland — EFFI ry. Lehdistötiedote. Helsinki 28.11.2002. http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2002-11-28.html (tarkastettu 2.9.2004).

[Virtanen, 2002] Teemupekka Virtanen, Tietosuoja luo yrityksen brandia. *Tietosuoja* **15**, 1 (2002), 17—19.

[Wallin ja Nurmi, 1991] Anna-Riitta Wallin ja Pekka Nurmi, *Tietosuojalainsäädäntö. Henkilörekisterilaki ja siihen liittyvät säädökset.* 2. uudistettu painos. Gummerus, Jyväskylä, 1992.

[Wallin, 1998] Anna-Riitta Wallin, Julkisuus- ja salassapitolainsäädäntö uudistuu. *Tietosuoja* **11**, 2 (1998), 4—8.